

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平6-162059

(43)公開日 平成6年(1994)6月10日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/30	M	6798-5L		
	3 6 0	6798-5L		
G 0 7 F 19/00		8513-3E	G 0 7 D 9/ 00	4 7 6

審査請求 有 請求項の数108(全 113 頁)

(21)出願番号 特願平4-330971

(22)出願日 平成4年(1992)11月16日

(31)優先権主張番号 07/794112

(32)優先日 1991年11月15日

(33)優先権主張国 米国(US)

(71)出願人 592255202

シティーバンク エヌ、エー、
Citibank, N. A.
アメリカ合衆国、ニューヨーク州 10043、
ニューヨーク、パーク アベニュー 399

(72)発明者 ショルム エス、ローゼン

アメリカ合衆国、ニューヨーク州 10024、
ニューヨーク、ウエスト エイティシック
ス ストリート 10、アパートメント
7エー

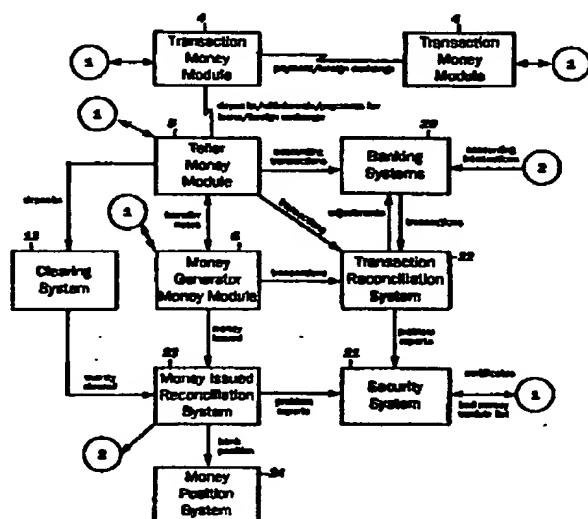
(74)代理人 弁理士 新実 健郎 (外1名)

(54)【発明の名称】 電子通貨システム

(57)【要約】 (修正有)

【目的】 通常の現金と交換可能で、かつ一般に受入れ可能な電子マネーを用いる完全な電子通貨システムを提供することである。

【構成】 営業性預金に支持された電子通貨を含む電子マネーを加入者に対して発生及び発行するための金銭発生装置に結合された発行銀行1と、電子マネーを受け入れ、かつ分配するコルレス銀行2と、電子マネーをストアし、参加銀行1、2のオンラインシステムとの間で金銭取引を実行する取引装置4と、取引装置4を発行銀行1及びコルレス銀行2に接続すること、及び発行銀行1とコルレス銀行2との間を接続することを実行する出納装置5と、システムの完全性を維持するための安全保障機構21及び通貨体系を監視し、かつ清算するための調整及び決済プロセス13、23を含むものである。



Network 28 (not shown)

Electronic Monetary System

【特許請求の範囲】

【請求項1】 銀行における預金上の請求を介して通常の貨幣と交換可能な電子通貨及び電子信用認可を含む電子マネーを具体化し、かつ維持するための電子通貨システムであって、

各々が電子マネー勘定手段を含む複数の発行手段と、前記電子マネーを発生するための発生手段と、前記発生手段への接続を形成し、かつ出納処理を実行するための複数の出納処理手段であって、互いに他の出納処理手段と接続可能であって、その出納処理として前記電子マネーの受入及び分配を行うことができるようにしたもの、前記発行手段の各々における前記電子マネー勘定を清算するとともに、前記発行手段により発行された前記電子マネーを清算するための決済手段、及び前記電子マネーを移転するための複数の取引手段であって、前記移転を前記取引手段間及び前記取引手段と前記出納処理手段との間で行うようにしたものを備えたことを特徴とする電子通貨システム。

【請求項2】 前記システムがさらに、複数のコルレス手段を含み、各コルレス手段が電子マネー勘定手段を有し、前記出納処理手段が他の出納処理手段との間で電子マネーの受入及び分配を含む取引を行うものであることを特徴とする請求項1記載のシステム。

【請求項3】 前記システムがさらに、前記電子通貨システムの安全性及び完全性を維持するための安全保障手段を含むことを特徴とする請求項1記載のシステム。

【請求項4】 前記システムがさらに、前記発生手段、前記出納処理手段、前記決済手段、前記取引手段及び前記安全保障手段相互間における通信リンクを提供するためのネットワーク手段を含むことを特徴とする請求項3記載のシステム。

【請求項5】 前記発生手段がさらに、複数の通貨において電子マネーを発生するものであることを特徴とする請求項3記載のシステム。

【請求項6】 前記システムがさらに、前記取引手段、前記出納処理手段、及び前記発生手段相互間において、安全にデータを伝達するための手段を含むことを特徴とする請求項1記載のシステム。

【請求項7】 前記データ伝達手段がさらに、前記電子マネーの複写又は不正操作から保護するために前記データを暗号化するものであることを特徴とする請求項6記載のシステム。

【請求項8】 前記発行手段の各々がさらに、前記各発行手段により発行された前記電子マネーを調整するための手段を含むことを特徴とする請求項1記載のシステム。

【請求項9】 前記発行手段の各々及び前記コルレス手段の各々がさらに、前記電子マネーの移転により生じた取引レコードを調整するための手段を含むことを特徴と

する請求項1記載のシステム。

【請求項10】 現金取引に代わる電子データ取引を実行するための方法であって、発生手段を用いて営業性預金及び貸出限度額により支持された経済的価値の電子的象徴を発生するための発生手段を提供するステップと、

前記経済的価値の電子的象徴を発生するステップと、出納処理手段を用いて前記発生された経済的価値の電子的象徴を受け入れるとともに、前記経済的価値の電子的象徴を発行するステップと、権限を有する利用者に対し経済的為替の電子的象徴を発行するステップと、

前記権限を有する利用者取引手段を提供して、前記経済的為替の電子的象徴を前記取引手段を有する他の権限を有する利用者及び前記出納処理手段に移転するステップ、及び前記経済的為替の電子的象徴を受入れ、かつ現金の支払に代えて前記取引手段を所持した他の権限を有する利用者及び前記出納処理手段に移転するステップを含むことを特徴とする電子データ取引の実行方法。

【請求項11】 前記方法がさらに、複数の前記発生手段を提供するステップを含むことを特徴とする請求項10記載の方法。

【請求項12】 前記方法がさらに、前記発生手段の各々からの前記経済的価値を表す電子的象徴の発行を記録するとともに、前記出納処理手段による前記経済的価値の電子的象徴の受入を記録するための勘定を提供するステップを含むことを特徴とする請求項11記載の方法。

【請求項13】 前記方法がさらに、前記勘定を清算するための清算処理を提供するステップを含むことを特徴とする請求項12記載の方法。

【請求項14】 前記方法がさらに、複数の前記発生手段を提供するステップを含むことを特徴とする請求項10記載の方法。

【請求項15】 前記方法がさらに、前記発生手段、前記出納処理手段及び前記取引手段相互間において、前記経済的価値の電子的象徴を安全に伝送するための安全保障手段を提供するステップを含むことを特徴とする請求項10記載の方法。

【請求項16】 前記方法がさらに、前記発生手段、前記出納処理手段、前記清算処理、前記取引手段、及び前記安全保障手段間における通信を行うためのネットワーク接続手段を提供するステップを含むことを特徴とする請求項10記載の方法。

【請求項17】 銀行における営業性預金又はにより支持された電子通貨電子的信用認可を含む電子マネーを用いた取引を提供するための電子通貨システムであって、前記電子マネーを発生するための手段と、

前記電子マネーを発行し、分配し、及び受け入れるための手段と、前記電子マネーを受入れ、ストアし、及び移転するため

の手段であって、それらの処理を他の同種の手段との間及び前記発行手段との間において実行するための手段を備えたことを特徴とする電子通貨システム。

【請求項18】 前記システムがさらに、その電子通貨システムの安全性及び完全性を維持するための手段を含むことを特徴とする請求項17記載のシステム。

【請求項19】 前記システムがさらに、前記発生手段、前記発行手段、前記受入手段、及び前記安全保障手段相互間における通信ネットワークを提供するための手段を含むことを特徴とする請求項18記載のシステム。

【請求項20】 前記システムがさらに、前記発行された電子マネーのレコード及び前記受入手段より前記発行手段に移転された前記電子マネーのレコードをストアするための会計データファイルを維持し、かつ処理するための手段を含むことを特徴とする請求項17記載のシステム。

【請求項21】 複数の加入者及び前記複数の加入者に対し通常の貨幣を金銭の電子的象徴と交換することにより、奉仕する少くとも1つの金融機関を有する通貨システムにおいて用いられるための金銭代行物たる電子的象徴であって、前記電子的象徴が、(1)代表される金銭的価値、(2)前記電子的象徴の発生源、及び(3)前記電子的象徴の有効性を支持するデータを含むデジタルフォームからなることを特徴とする金銭代行用の電子的象徴。

【請求項22】 前記電子的象徴が機能上銀行手形と等価なものとして用いられることを特徴とする請求項21記載の電子マネー。

【請求項23】 前記電子的象徴がその買戻しを否定されないように用いられるものであることを特徴とする請求項21記載の電子マネー。

【請求項24】 前記電子的象徴が通貨又は信用のいずれかを表すことができるようにしたことを特徴とする請求項21記載の電子マネー。

【請求項25】 前記データが前記電子的象徴の状態を確認するためのデータ表現を含むことを特徴とする請求項21記載の電子マネー。

【請求項26】 前記データが安全に記憶される形態をもち、かつ携帯可能な個人用プロセッサにおいて処理されるものであることを特徴とする請求項21記載の電子マネー。

【請求項27】 金銭の電子的象徴を用い、かつ少くとも1つの金融機関と前記金融機関により奉仕される加入者を含む通貨システムであって、各々が前記電子的象徴を代行される金額及び前記電子的象徴の有効性を支持するデータを含む機械読取可能なデジタル型において収容できるようにした複数の加入者プロセッサと、前記金融機関により用いられて前記加入者プロセッサと通信することにより、前記加入者プロセッサにストアさ

れた電子的象徴を前記金融機関に預金すること、又は前記加入者プロセッサに対し前記金融機関から前記電子的象徴を払い戻すことを可能にした処理手段とを備え、前記加入者プロセッサはさらに、加入者プロセッサ間において前記電子的象徴の交換を行うことができるようにするための通信及び処理機能を含むものであることを特徴とする通貨システム。

【請求項28】 前記金銭代行物としての電子的象徴が銀行手形と同等に機能するものとして用いられることを特徴とする請求項27記載のシステム。

【請求項29】 前記システムが、前記電子的象徴の有効性を支持することによりその処理を可能にするための証明資源を含むことを特徴とする請求項27記載のシステム。

【請求項30】 前記システム中に複数の金融機関と、前記複数の金融機関及び前記加入者プロセッサ相互間で清算処理を行うための決済機関が含まれることを特徴とする請求項27記載のシステム。

【請求項31】 前記加入者プロセッサ中にストアされた前記データが前記電子的象徴の状態を確認するためのデータ表現を含むことを特徴とする請求項27記載のシステム。

【請求項32】 前記加入者プロセッサ中にストアされた前記電子的象徴が、前記金融機関との取引中において更新された電子的象徴と置換されるようにしたことを特徴とする請求項27記載のシステム。

【請求項33】 経済的価値を安全確実に交換するために電子媒体を用いる通貨システムであって、信用認可の電子的象徴、及び銀行における営業性預金により支持された通貨の電子的象徴と、

前記信用の電子的象徴及び前記通貨の電子的象徴を発生するための手段と、

前記発生手段に結合されて前記信用及び通貨の前記電子的象徴を発行し、分配し、及び受け入れるための出納手段、及び前記信用及び通貨の電子的象徴をストアし、かつ移転するための取引手段であって、前記移転を他の取引手段との間及び前記手段と前記出納手段との間において実行することができるようにしたものを備えたことを特徴とする通貨システム。

【請求項34】 前記システムがさらに、その通貨システムの安全性及び完全性を維持するための安全保障手段を含むことを特徴とする請求項33記載のシステム。

【請求項35】 前記安全保障手段がさらに、前記取引手段間における前記信用及び通貨の電子的象徴の移転可能性に時間的制限を与えるものであることを特徴とする請求項34記載のシステム。

【請求項36】 前記発生手段、前記出納手段及び前記取引手段の各々が個々に認識番号を有することを特徴とする請求項34記載のシステム。

【請求項37】 前記安全保障手段がさらに、前記発生

手段、前記出納手段及び前記取引手段の各々における前記認識番号の安全な証明を提供するための証明手段を含むことを特徴とする請求項36記載のシステム。

【請求項38】 前記証明がさらに、前記発生手段、前記出納手段又は前記取引手段のうちの他のものによるその受入可能性の時間限度を含むようにしたことを特徴とする請求項37記載のシステム。

【請求項39】 前記安全保障手段がさらに、前記発生手段、前記出納手段、前記取引手段、及び前記安全保障手段の相互間における通信リンクを提供するためのネットワーク接続手段を含むことを特徴とする請求項34記載のシステム。

【請求項40】 前記ネットワーク接続手段がさらに、このネットワーク接続手段を横切って通信メッセージを接続し、管理し、及び誘導するためのネットワーク奉仕手段を含むことを特徴とする請求項39記載のシステム。

【請求項41】 前記発生手段がさらに、信用及び通貨のための電子的象徴を複数の通貨単位について発生するものであることを特徴とする請求項33記載のシステム。

【請求項42】 前記信用及び通貨のための電子的象徴が経済的価値として受け入れられるとともに、それらの初期の経済的価値以下の価値において通信及び移転されるものであることを特徴とする請求項33記載のシステム。

【請求項43】 前記信用の電子的象徴が前記取引手段により1回だけ移転されるようにしたこと特徴とする請求項42記載のシステム。

【請求項44】 前記発生手段がさらに、前記信用及び通貨のための電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項33記載のシステム。

【請求項45】 前記出納手段がさらに、前記信用及び通貨のための電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項33記載のシステム。

【請求項46】 前記取引手段がさらに、前記信用及び通貨のための電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項33記載のシステム。

【請求項47】 前記信用及び通貨のための電子的象徴が、

- (1) 通貨又は信用のいずれを表しているか、
- (2) その移転可能性の時間限度、
- (3) その経済的価値と前記電子的象徴をすでに記憶した他の取引手段、
- (4) 前記発生手段の前記デジタル署名、
- (5) 前記出納手段の前記デジタル署名、
- (6) 前記他の取引手段における前記デジタル署

名、

- (7) 前記他の取引手段における前記証明、
- (8) 前記出納手段における前記証明、
- (9) 前記発生取引手段の前記証明、
- (10) 前記通貨又は信用のための電子的象徴の認識番号、

の表記を含むものであることを特徴とする請求項43記載のシステム。

【請求項48】 前記発生手段、前記出納手段、及び前記取引手段が不正行為防止用ハウジングに収納されたプログラムブルデータ処理装置から構成されたものであることを特徴とする請求項33記載のシステム。

【請求項49】 前記発生手段、前記出納手段及び前記取引手段がコンピュータのモジュラ型共同プロセッサとして機能するように構成されたことを特徴とする請求項48記載のシステム。

【請求項50】 前記システムがさらに、2以上の手段により発行された信用及び通貨のための前記電子的象徴を清算するための手段を含むことを特徴とする請求項33記載のシステム。

【請求項51】 少くとも1つの金融機関により提供される通貨の電子的象徴又は信用の電子的象徴を用いる方法であって、前記金融機関が前記電子的象徴を発生する手段と、前記電子的象徴を発行し、かつ受け入れるとともに前記機関による加入者への奉仕を実行するための出納手段を有するものであり、前記方法が、

(1) 営業性預金により支持された通貨のための前記電子的象徴を発生するか、又は信用認可のための前記電子的象徴を発生するステップと、

(2) 前記通貨又は信用のための電子的象徴を前記加入者に対して発行するとともに、前記金融機関における前記出納手段から受け入れるステップ、及び

(3) 前記加入者に対し、前記通貨又は信用のために前記発行された電子的象徴を受け入れるとともに、その電子的象徴を前記取引手段を有する他の加入者及び前記出納手段に移転するための取引手段を提供するステップを含むことを特徴とする通貨又は信用のための電子的象徴を用いる方法。

【請求項52】 前記方法がさらに、前記通貨又は信用のための前記電子的象徴にデジタルサインを施し、これによってその複製もしくは変造等を防止して信頼性及び安全性を提供するステップを含むことを特徴とする請求項51記載の方法。

【請求項53】 前記方法がさらに、前記通貨又は信用のための前記電子的象徴が前記取引手段間において移転可能な時間周期を制限するステップを含むことを特徴とする請求項52記載の方法。

【請求項54】 前記方法がさらに、前記取引手段が前記金融機関と取引する限り、前記取引手段中にストアされた通貨を表す電子的象徴のすべてを取り除くステップ

と、移転可能性の時間限度を更新した通貨を表す新たな電子通貨を発生するステップ、及び前記取引手段において前記最初の通貨を表す電子的象徴を置換するステップを含むことを特徴とする請求項53記載の方法。

【請求項55】 前記方法がさらに、前記取引手段が前記信用の電子的象徴を発行する金融機関と取引するときに、前記取引手段中にストアされた信用を表す前記電子的象徴のすべてを取り除くステップと、移転可能な時間限度を更新した新たな信用を表す電子的象徴を発生するステップ、及び前記取引手段において前記最初の信用を表す電子的象徴を置換するステップを含むことを特徴とする請求項53記載の方法。

【請求項56】 前記方法がさらに、前記金融機関により発行された通貨又は信用を表す前記電子的象徴のレコードを清算し、かつ維持するステップを含むことを特徴とする請求項51記載の方法。

【請求項57】 前記方法がさらに、前記発生手段、前記出納手段及び前記取引手段の各々に対し新規の認識番号を提供するステップを含むことを特徴とする請求項51記載の方法。

【請求項58】 前記方法がさらに、前記発生手段、前記出納手段及び前記取引手段の各々における前記認識番号の有効性を確認するステップを含むことを特徴とする請求項57記載の方法。

【請求項59】 前記方法がさらに、前記発生手段、前記出納手段及び前記取引手段の各々における所定時間内での前記認識番号の有効性を確認するステップを含むことを特徴とする請求項58記載の方法。

【請求項60】 前記方法がさらに、前記発生手段、前記出納手段及び前記取引手段の各々に対し、何らかの理由で好ましくない出納手段、発生手段、又は取引手段のリストを提供するステップを含むことを特徴とする請求項59記載の方法。

【請求項61】 前記方法がさらに、複数の異なった通貨単位について信用及び通貨を表す前記電子的象徴を発生するステップを含むことを特徴とする請求項51記載の方法。

【請求項62】 前記方法がさらに、前記金融機関において前記通貨又は信用を表す電子的象徴の分配、及び何らかの金融取引後における各金融機関の債務を監視するための会計構造を提供するステップを含むことを特徴とする請求項51記載の方法。

【請求項63】 前記方法がさらに、前記金融機関の各々において前記加入者に関連する口座のための個々のリストを前記取引手段にストアするステップを含むことを特徴とする請求項62記載の方法。

【請求項64】 前記方法がさらに、コルレス金融機関のデジタル署名により前記銀行口座のリストの各々にデジタル署名し、これによって前記口座に対する無権限者のアクセスを防止するためのステップを含むことを

特徴とする請求項63記載の方法。

【請求項65】 前記方法がさらに、前記金融機関において前記加入者に対し前記口座に関する金銭の引出及び預金、貸付に対する支払、及び通貨の交換を含む銀行サービスを提供するステップを含むことを特徴とする請求項62記載の方法。

【請求項66】 前記方法がさらに、前記取引手段により実行された取引のレコードを維持するとともに、前記取引手段内の前記レコードをストアするステップを含むものであり、前記取引レコードが移転日、移転金額、前記通貨又は信用を表す電子的象徴を発行する金融機関の認識番号、前記取引に含まれる他の取引手段の認識番号、及び移転された通貨又は信用を表す電子的象徴の認識番号の表記を含むものであることを特徴とする請求項57記載の方法。

【請求項67】 前記方法がさらに、前記金融機関における前記取引レコードの複製を維持するステップと、前記手段のいずれかとの取引後において前記取引手段の各々に対する前記レコードを更新するステップを含むことを特徴とする請求項66記載の方法。

【請求項68】 前記方法がさらに、前記取引手段の前記取引レコードを、前記通貨及び信用を表す電子的象徴の清算により発生した取引レコードを用いて調整するステップを含むことを特徴とする請求項67記載の方法。

【請求項69】 前記方法がさらに、前記取引手段の前記取引レコードを前記通貨及び信用を表す電子的象徴の清算により発生した取引レコードと比較することにより、紛失し、又は盗難にあった取引手段中にストアされた通貨及び信用を表す電子的象徴の真の値を判定し、前記失われた値の正確な置換を行うステップを含むことを特徴とする請求項68記載の方法。

【請求項70】 前記方法がさらに、前記金融機関及び前記取引手段を互いに接続する通信ネットワークを提供するステップを含むことを特徴とする請求項51記載の方法。

【請求項71】 銀行における営業性預金により支持された通貨を表す電子的象徴を用いて取引を行うための電子通貨システムであって、
前記通貨を表す電子的象徴を発生するための手段と、
前記通貨を表す電子的象徴を発行し、かつ分配するための出納手段と、
前記通貨を表す電子的象徴をストアし、かつ移転するための取引手段であって、前記移転を他の取引手段との間において実行する手段を備えたことを特徴とする電子通貨システム。

【請求項72】 信用認可を表す電子的象徴を用いて取引を行うための電子通貨システムであって、
前記信用を表す電子的象徴を発生するための手段と、
前記信用を表す電子的象徴を発行し、かつ分配するための出納手段と、

10

20

30

40

50

前記信用を表す電子的象徴をストアし、かつ移転するための取引手段であって、前記移転を他の取引手段との間及び前記取引手段と前記出納手段との間において実行する手段を備えたことを特徴とする電子通貨システム。

【請求項73】 前記システムがさらに、その電子通貨システムの安全性及び完全性を維持するための安全保障手段を含むことを特徴とする請求項71又は72記載のシステム。

【請求項74】 前記システムがさらに、前記発生手段、前記出納手段、前記取引手段、及び前記安全保障手段間における通信ネットワークを提供するための手段を含むことを特徴とする請求項71又は72記載のシステム。

【請求項75】 前記システムがさらに、前記発生手段により発行された通貨又は信用を表す電子的象徴のレコード、及び前記取引手段により前記出納手段に移転された前記通貨又は信用を表す電子的象徴のレコードをストアするための口座データファイルを維持し、かつ処理するための手段を含むことを特徴とする請求項71又は72記載のシステム。

【請求項76】 前記安全保障手段がさらに、前記信用を表す電子的象徴及び前記通貨を表す電子的象徴の前記取引手段間における移転可能性の時間限度を設定するものであることを特徴とする請求項73記載のシステム。

【請求項77】 前記発生手段、前記出納手段及び前記取引手段の各々が個々に認識番号を有することを特徴とする請求項73記載のシステム。

【請求項78】 前記電子通貨システムの安全性を維持するための手段がさらに、前記発生手段、前記出納手段及び前記取引手段の各認識番号の独自の証明を行うための証明手段を含むことを特徴とする請求項77記載のシステム。

【請求項79】 前記証明がさらに、前記発生手段、前記出納手段もしくは前記取引手段のうちの他のものによるその受入可能な時間限度を含むことを特徴とする請求項78記載のシステム。

【請求項80】 前記ネットワーク接続手段がさらに、その手段を通じて通信メッセージを接続し、管理し、及び誘導するためのネットワーク奉仕手段を含むことを特徴とする請求項74記載のシステム。

【請求項81】 前記発生手段がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項71又は72記載のシステム。

【請求項82】 前記出納手段がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項71又は72記載のシステム。

【請求項83】 前記取引手段がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項71又は72記載のシステム。

【請求項84】 前記通貨を表す電子的象徴又は前記信用を表す電子的象徴が経済的価値として受け入れられるものであることを特徴とする請求項71又は72記載のシステム。

10 【請求項85】 前記通貨を表す電子的象徴又は前記信用を表す電子的象徴が発生された初期の経済的価値に等しいか、又はそれ以下の値において通信及び移転されることを特徴とする請求項71又は72記載のシステム。

【請求項86】 前記信用を表す電子的象徴が前記取引手段により1回だけ移転可能であることを特徴とする請求項85記載のシステム。

【請求項87】 前記通貨を表す電子的象徴又は前記信用を表す電子的象徴がさらに、

20 (1) その象徴が通貨又は信用のいずれを表しているか、

(2) 前記移転可能なその時間限度、及び

(3) その経済的価値

からなる表記を含むことを特徴とする請求項71又は72記載のシステム。

【請求項88】 前記表記がさらに、

(1) 前記電子的象徴をすでにストアした他の発生手段、出納手段及び取引手段に関する表記、

(2) 前記他の取引手段の証明、

(3) 前記出納手段の証明、及び

30 (4) 前記発生手段の証明

を含むことを特徴とする請求項87記載のシステム。

【請求項89】 前記表記がさらに、

(1) 前記発生手段の前記デジタル署名、

(2) 前記出納手段の前記デジタル署名、及び

(3) 前記他の取引手段における前記デジタル署名の表記を含むことを特徴とする請求項88記載のシステム。

40 【請求項90】 前記発生手段、前記出納手段、及び前記取引手段が各々不正行為防止用ハウジングに収納されたプログラマブル処理装置からなることを特徴とする請求項71又は72記載のシステム。

【請求項91】 前記発生手段、前記出納手段、及び前記取引手段が汎用コンピュータのモジュラ型共同プロセッサとして機能するものであることを特徴とする請求項90記載のシステム。

【請求項92】 前記汎用コンピュータが、携帯用コンピュータからなることを特徴とする請求項91記載のシステム。

50 【請求項93】 前記汎用コンピュータがさらに、パーソナルコンピュータからなることを特徴とする請求項9

11

1記載のシステム。

【請求項94】 前記汎用コンピュータが、ワークステーションコンピュータからなることを特徴とする請求項91記載のシステム。

【請求項95】 前記汎用コンピュータがさらに、メインフレームコンピュータからなることを特徴とする請求項91記載のシステム。

【請求項96】 前記汎用コンピュータがさらに、ミニコンピュータからなることを特徴とする請求項91記載のシステム。

【請求項97】 前記汎用コンピュータがさらに、販売時点情報管理用コンピュータターミナルからなることを特徴とする請求項91記載のシステム。

【請求項98】 前記汎用コンピュータがさらに、インテリジェント型電話機からなることを特徴とする請求項91記載のシステム。

【請求項99】 前記プログラマブル処理装置の各々がさらに、他の好ましくないプログラマブル処理装置のリストを含んでいることを特徴とする請求項90記載のシステム。

【請求項100】 前記システムがさらに、2以上の出納手段により発行された信用及び通貨を表す電子的象徴を清算するための手段を含むことを特徴とする請求項71又は72記載のシステム。

【請求項101】 前記金融機関がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴の分配と、いずれかの金融取引後における各金融機関の負債を監視するための会計構造を含むことを特徴とする請求項71又は72記載のシステム。

【請求項102】 前記取引手段中における前記プログラマブル処理装置がさらに、前記異なった金融機関の各々において維持された前記取引手段の所有者に関する個々の口座リストを含むことを特徴とする請求項90記載のシステム。

【請求項103】 前記口座リストの各々がさらに、前記口座を維持する金融機関のデジタル署名を含むことにより、前記口座への無権限者のアクセスを防止することを特徴とする請求項102記載のシステム。

【請求項104】 前記発生手段がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴を複数の通貨単位において発生するものであることを特徴とする請求項71又は72記載のシステム。

【請求項105】 前記プログラマブル処理装置の各々が前記金融機関のいずれとも何らの関係を有しない個人であって、その存在認識に関して匿名性を維持したものであることにより所有され、かつ制御されるものであることを特徴とする請求項90記載のシステム。

【請求項106】 前記プログラマブル処理装置を所有する前記個人が前記プログラマブル処理装置を占有することにより、無権限者によるその使用を禁止するように

12

したことを特徴とする請求項105記載のシステム。

【請求項107】 前記プログラマブル処理装置を所有する個人が自然人であることを特徴とする請求項105記載のシステム。

【請求項108】 前記プログラマブル処理装置を所有する個人が事業体であることを特徴とする請求項105記載のシステム。

【発明の詳細な説明】

【0001】

10 【産業上の利用分野】本発明は、現金、小切手、クレジットカード及びデビットカード（借方カード）に対する為替取引の交換媒体などのような電子マネー支払方式、及び電子的資金トランスファを実行するための電子通貨システムに関するものである。電子通貨システムは貨幣、小切手、カード支払方式、及び電子的資金トランスファシステムの混成物であり、これらのシステムの利点の多くを維持しながら、それらのシステムに固有の制約をそれほど受けないものである。この電子通貨システムはシステム加入者により経済的価値として一般的に受け入れられ、かつ交換されるように設計された電子的な金銭代行物を利用する。

【0002】

20 【従来の技術】今日の経済情勢では、毎年個人及び団体間で取引される貨幣の総量は約3500億単位である。この貨幣取引の大量利用は購入、飲食、及び預金口座への預入及び引出などのような個々の経済取引の自動化を制限する。個々の現金取引は正確な金額を有すること、又はそのための両替もしくは現金化を行わなければならないという負担がある。さらに、紙幣及び硬貨の取扱い

30 は不便であり、個人及び金融機関のいずれにとってもそのコスト及び時間消費を無視し得ない。
【0003】小切手は当座勘定において許される範囲までの金額を書き込めるものであるが、小切手は移転性を大きく制約されるとともに、物的明細（フィジカルインベントリー）から供給されなければならない。紙券小切手システムは現金移転の制約からそれほど大きな自由をえられるものではなく、通貨を扱うという不利益の多くを同様にもっており、しかも、小切手処理に関する固有の時間遅れをも考慮しなければならない。このため、そのような為替取引はより低いコストにおいてより多くの利便を生み出す新たな方法を要求し、しかも、安全性の改良を追求してきた。

40 【0004】自動化技術はこれらの特質の幾つかを、大取引のためにコンピュータ化された電子資金移転（EFT）システムにより実現した。電子資金移転とは、基本的に銀行体系の中央コンピュータ処理を通じて実現される価値交換のプロセスである。このEFTサービスは基本的に大商業組織によって用いられる電子“小切手”を利用した支払の移転である。

50 【0005】自動化されたクリアリング・ハウス（AC

H：手形交換所）及び販売時点情報管理（POS）システムは、近年実質的ベースにおいて小売及び商業組織により用いられるようになった電子資金移転システムの例である。しかしながら、これらのタイプのEFTシステムを通じて行われる支払は、それらが銀行体系なしでは達成できないという制約を受け、さらには、ACH取引は通常、営業時間外に行うことができないものである。

【0006】内国銀行の手形支払サービスは支払を行う各個人に利用される電子資金移転システムの例である。しばしば、内国銀行の先導の下で、顧客は少数である。支払サービスを提供する銀行において、パーソナルコンピュータを用いた電話回線による口座振替及び情報通信は、その銀行の顧客の1%にも満たない利用客にそのサービスを行っている。そのような内国銀行業務が成功しなかった理由は、顧客がこのタイプのシステムにおいて、必要に応じた金銭の預金及び引き出しを行うことができないという理由による。

【0007】最近のFETシステム、クレジットカード又はデビットカードは、商人の口座と顧客の口座との間などで金銭を移転するためにオンラインシステムを通じて利用されるが、それは銀行体系の部外者が一般的に受け入れられる経済的価値の移転を行う自動取引システムとしての機能を満足することはできない。

【0008】自動化されたより便利な取引システムとして、移転を仲介するために銀行体系を必要とすることなく、何らかの経済的価値を分配することができるようなシステムを実施するため、現在一般の趨勢はオフライン電子資金移転に向かっている。例えば、旧来の貨幣及び小切手タイプの支払方式に対する代替物として、キャッシュレス支払行為に用いることができる、ある種の“電子マネー”について多くの考えが提案されてきた。例えば、「電子キャッシュ実施方法及び装置」に関する米国特許第4977595号及び「モジュラ型資金移転方式」に関する米国特許第4305059号等がこれに当たる。

【0009】比較的良好に知られた技術としては、所定の金額のために購入され、かつそこから特定の目的のために予納値が割り引かれるという磁気ストライプカードがある。経済的価値が放出されると、そのカードは廃棄される。他の例としては、やはり特定の目的のために割り引かれる値に対応した情報を繰返しストアすることができる記憶カード、いわゆるスマートカードがある。

【0010】しかしながら、これらの既提案システムは金銭として銀行預金の重要性を完全に認識することの不足、及び発行可能で、かつ一般に受入可能な通貨代行物を何らかの形態において裏書きすることが必要であるという不都合が存在する。したがって、これら従来のシステムにおいては、電子的又は紙券的いずれかの経済的価値の象徴はそれらの価値に対向するような等価的な負担義務の裏付けなしに発行される。

【0011】したがって、これまでに提案されたペーパーレス支払方式においては、加入者が何らかの仲介システムを経ることなく、互いに電子資金又は金銭を移転することができるように自動化されているだけでなく、電子マネーによって表わされた価値を発生するとともに、システム内で貨幣残高を維持するために、システムに含まれる銀行及び金融機関の電子マネー勘定を清算できるような多目的電子通貨システムを実現できるものは存在しなかったと言える。

10 【0012】かくして、一般の支払者が銀行体系の仲介を受けることなく為替取引的な支払を行うことができ、かつ個々に支払工程を制御するようなシステムが特に必要とされる。さらに、経済的為替システムは、大組織がいかなるサイズにおける商業的支払のためにも用いることができること、及び現在のEFTシステムに関する制約を受けないということが要求される。

【0013】

20 【発明の目的】したがって、本発明の一つの目的は、通常の現金と交換可能であり、かつ一般に受け入れられる電子マネーを用いた完全な電子通貨システムを提供することである。

【0014】本発明の別の目的は、加入者間、金融機関間、及び加入者と金融機関との間における通貨及び信用を含む経済的価値を確実に移転する方法を提供することである。

【0015】本発明のさらに別の目的は、多目的ペーパーレス支払方式を提供し、これによって取引が加入者間においてオンライン及びオフラインのいずれにおいても実施されるようにしたものである。

30 【0016】本発明のさらに別の目的は、オフライン装置への支払の多くをオフロードとすることにより、中央電子資金移転システムのコストを低下させるようにした支払方式を提供することである。

【0017】本発明のさらに別の目的は、紙幣、小切手、及び硬貨を管理する制度的コストを低下させるための廉価な電子移転システムを提供することである。

40 【0018】本発明のさらに別の目的は、一般大衆メンバー間、一般大衆メンバーと商業組織との間及び商業組織間において金銭の移転をリアルタイムで信頼性よく確実に実行できるような利用者親展型電子支払方式を提供することである。

【0019】本発明のさらに別の目的は、近年普及しつつある取引銀行サービス方式を含む広汎なデータ処理及びデータ通信システムと一体化されるようにした経済的価値の預金及び引出方式を提供することである。

【0020】本発明のさらに別の目的は、多種通貨型の電子マネーを利用する電子通貨システムを提供することである。

50 【0021】本発明のさらに別の目的は、考えられる如何なる額面単位の取引においても安全にその経済的価値

を移転するためのシステムを提供することである。

【0022】本発明のいま一つ目的は、交換可能で容易に移転可能であり、かつ償還可能な経済的為替媒体であって、再使用や複写及び偽造の危険がないものを提供することである。

【0023】

【発明の概要】以上述べたことを実現するため、本発明の方法及び装置はその電子通貨システムの一形態において次の諸要素を採用したものである。

(1) 第一の要素は銀行又は金融機関であり、これらは営業性預金により裏付けられた電子通貨及び電子信用認可を含む電子マネーを加入者に対して発行するための金銭発生装置に結合される。(2) 第二の要素はコルレス銀行であり、これらは電子マネーを受入及び分配するものである。(3) 第三の要素は複数の取引装置であり、これらは加入者により電子マネーをストアし、関連銀行のオンラインシステムにより金銭取引を実行し、又は電子マネーを他の同様な取引装置を用いてオンライン処理において交換するために用いられる。(4) 第四の要素は発行銀行及びコルレス銀行に関連する出納装置であり、これらは発行銀行及びコルレス銀行に対して取引装置を処理し、かつ接続するとともに、発行銀行及びコルレス銀行間を接続するものである。(5) 第五の要素は異なった発行銀行の電子マネー勘定を清算するための決済銀行(クリアリング・バンク)である。(6) 第六の要素はシステムのすべての要素に対する通信サービスを行うためのデータ通信ネットワークである。(7) 最後に、第七の要素はシステムの完全性を維持するとともに、システム内での偽造及び不正行為を検出するための安全保障機構である。

【0024】好ましい実施例において、金銭発生装置、取引装置、及び出納装置の各機能は不正防止コンピュータハードウェア及びアプリケーションソフトウェアモジュールの組合せにより達成され、それらはネットワーク上に一括される。情報は秘密の形態で伝達され、無権限の調査行為から保護される。電子マネーは変造又は偽造から保護されるように信頼すべきデジタル署名により伝達される。

【0025】これらの装置により、為替取引された電子マネーは通貨又は信用の電子的象徴となり得る。電子通貨の重要な局面は、それが銀行券と等価であり、かつ発行銀行における預金上の請求を通じて在来の紙幣と相互に交換できるものであるが、それは発行銀行及びコルレス銀行のいずれにおいても引出又は預金を行うことができる。しかしながら、電子通貨は発行銀行のみが発信できるものであり、その受戻しの責任を負わされる。

【0026】発行銀行は後に銀行間決済を利用して、今日の銀行産業において一般に行われている通り通貨残高を維持する。

【0027】本発明の電子マネー象徴は、一般に受入及

び代替可能であるとともに発行銀行から確実に償還可能なものである。すなわち、それらは金銭取引の特徴を有するものである。電子通貨システムの完全性を保持するため、電子マネーの各為替取引は信用又は通貨の貨幣単位(すなわち、ドル、円、その他)、その信用又は通貨の貨幣単位による金額、電子的信用又は通貨を発行する銀行、及び幾つかのデジタル署名を識別するデータを他の情報とともに含むものである。

【0028】

【発明の要約】要約すれば、本発明はその目的に従って次のような構成を提供する。次の要約においては、幾つかの単純化及び省略がなされ、本発明の幾つかの局面を経済的に導入しようとするものであるが、もちろん本発明をその範囲のみに限定するものではない。

【0029】本発明の概略構成によれば、電子通貨システムは現金取引の代わりに銀行における営業性預金により裏付けられる電子通貨、及び電子信用認可を含む電子マネー信用取引を行うものである。本発明は、電子マネーを発生するための金銭モジュール、並びに他の受入金銭モジュール間、及び受入金銭モジュールと発行金銭モジュールとの間で電子マネーを受入れ、ストアし、及び移転するための金銭モジュールを備えている。

【0030】本発明の別の局面によれば、電子通貨システムは銀行における預金上の請求を通じて在来通貨と相互交換可能な電子通貨及び電子信用認可を含む電子マネー手段を具体化し、及び維持するものである。

【0031】システムは複数の発行銀行と、電子マネーを発生する発生モジュールと、発生モジュールに結合された出納モジュールであって、出納チェック処理を行い、電子マネーの受入及び分配を含むその処理を他の出納モジュールに接続するものと、電子通貨システム全体の完全性を提供するための安全保障システムと、個々に分離した発行銀行の電子マネー口座を清算させるとともに、発行銀行によって発行された電子マネーを支払うための決済処理、並びに処理モジュール間及び処理モジュールと出納モジュールとの間において、電子マネーを移転するために、権限を有する利用者により処理される複数の取引モジュールを含むものである。

【0032】本発明のさらに別に局面において、発生モジュール、取引モジュール、及び出納モジュールの機能は一括してネットワーク接続される不正防止型コンピュータハードウェア及びアプリケーションソフトウェアの結合により達成されるであろう。

【0033】これらのモジュールによって為替取引された電子マネーは発行銀行における営業性預金口座によって支持(裏付け)された通貨又は信用認可の電子的象徴であり、それはデジタル署名により無権限者の変造又は偽造から保護されるように送信される。好ましい実施例において、偽造又は不正行為からの保護はモジュール及び電子マネーの個々の単位を周期的に更新するように

要求することによっても達せられる。誤ったモジュール又は偽造電子マネーはそれらが発見されるや否や、直ちに流通体系から除去されることができる。

【0034】略述すれば、電子通貨システムの処理は本発明に従って次の各ステップを含むものである。

(1) 発生モジュールにおいて、営業性預金又は貸出限度額によって支持された経済的価値の電子的象徴を発生させるステップ、(2) 出納モジュールにおいて、発生した経済的価値の電子的象徴を受け入れるとともに、経済的価値の電子的象徴を発行するステップ、

(3) 権限を有する利用者の取引モジュールにおいて、前記経済的価値の電子的象徴を受入れ、取引モジュールを所持した他の権限を有する利用者及び前記出納処理モジュールに移転するステップ、(4) 前記経済的価値の電子的象徴を受入れて、取引モジュールを有する他の権限を有する利用者及び前記出納モジュールに移転するステップ、及び(5) 安全保障システムにおいて、前記経済的価値の電子的象徴を発生モジュール、出納モジュール及び取引モジュール間において安全に移転できるようにするステップ、である。

【0035】

【好ましい実施例の説明】本発明は、確実かつ信頼性よく経済的価値を交換するために電子メディアを用いる改良された通貨システムを意図したものである。システムは新規のデータ処理システムに、他の手続を一体化することにより実現され、世界的規模における銀行体系に組み込むことができる。

【0036】この明細書を通じて、“電子マネー”は略号“E-M”により表現されることがある。さらに、“銀行”という用語は本発明のシステムに関連する銀行、金融機関等を表すために用いられる。

【0037】図面を参照するに際し、同一数字は同一の構成要素を指すものとし、図1においては、好ましい実施例の概略がブロック形態において示されている。図1には、システム要素の一般的関係が示されている。システムは各々金銭出納モジュール5及び金銭発生モジュール6を有する発行銀行1、各々金銭出納モジュール5を有するコルレス銀行2、電子マネー決済銀行3、証明機関28及びシステム加入者に所持された複数の金銭取引モジュール4を含んでいる。

【0038】電子手形11は電子マネーを移転するための媒体であり、それは発行銀行1毎に金銭発生モジュール6により発生される。これらの電子手形11は金銭出納モジュール5により、金銭取引モジュール4を利用する加入者に伝達される。電子手形11は通貨又は信用認可の代行物である。安全のため、すべての電子手形11は所定の期間後は期限切れとなる。期限切れとなった電子手形11は関連銀行において、それらが移転されるまでに更新されたものについて買取られなければならない。

【0039】発行銀行1は電子手形11を発生し、かつ分配するものであり、それらの買取の責任を負うものである。発行銀行1は他の金銭モジュールのための預金、引出、ローンに対する支払及び質問を実行する。

【0040】コルレス銀行2は発行銀行1において維持される口座を通じて電子マネーを分配する関連銀行であるが、それ自身何らの電子マネーを発生するものでもない。好ましい実施例において、コルレス銀行2は何らの電子マネーをも発生できないため、それは発行銀行1において維持される口座からの電子マネー要求をリアルタイムで処理しなければならない。これは加入者がコルレス銀行2において電子マネーを引き出そうと望む限り必要なことである。

【0041】逆に、コルレス銀行2は加入者によって預けられたすべての電子マネーをそのコルレス銀行2が発行銀行1に維持する口座に預金する。これらの口座については後に詳述する。コルレス銀行2は発行銀行1と同様、預金の引出、ローンへの支払及び銀行の質問を実行する。

【0042】発行銀行1は、通貨単位についてはその銀行が発生しないという意味においてコルレス銀行2と同じである。例えば、電子ドル手形11のための発行銀行1は他の銀行によって発行された円、マルク、その他の電子手形11については、コルレス銀行2となる。

【0043】さらに、留意すべきこととして、本発明のシステムは、コルレス銀行2なしで機能することもできる。例えば、加入者は預金又は引出等を行うとき、彼の発行銀行1と直接通信することによりコルレス銀行2を利用せずに済ませることができる。コルレス銀行2はシステムの利用範囲の拡散という目的のために好ましい実施例に含まれるのであり、ある種の銀行体系において固有の危険性、すなわち銀行発行マネーの衰弱(collapse)による危険を減少させるものである。

【0044】決済銀行3は2以上の銀行が電子マネーを発行するときに利用される。本発明によれば、それは2以上の銀行が電子マネーを発行するであろうとの予測に基づくものである。したがって、決済銀行3は発行銀行1のために預金された電子マネーを決済して口座の清算を保障するために組み入れられる。決済銀行3はシステム中の各発行銀行1毎に営業性預金勘定を維持するものである。

【0045】証明機関28はシステム安全性のための中央機関である。それは各金銭モジュールに対する証明を発行することにより、ある時間周期だけ金銭モジュールの有効性を保証するという手続を提供する。金銭モジュールは他の金銭モジュール4、5、6と取引することができるように有効性を保証されなければならない。

【0046】保証期間が過ぎるまでにその保証は更新され、加入者が継続して彼の金銭取引モジュール4を使用

できるようにしなければならない。この手順はシステム利用者が証明機関28と定期的に接触できるようにして達せられる。

【0047】この定期的接触はシステムの金銭モジュールによる不正行為が検出されたとき、速やかに応答することを可能にする。このため、証明機関28は他の金銭モジュールに対して違法な又は妥当な状態にある金銭モジュールのリストを提供し、これによって違法な他人との取引が阻止される。

【0048】図1に示された要素は図2に示されたシステムの機能的配列を参照することにより最もよく理解される。図2に示す通り、好ましい実施例は現在の銀行体系に次の付加的要素を補充するものである。すなわち、複数の金銭取引モジュール4と、金銭出納モジュール5と、電子手形11（金銭）を発生、移転、及びストアするための金銭発生モジュール6と、銀行が発行した通貨及び信用の勘定を決済するための決済システム13と、電子手形11の完全性を維持するための安全保障システム21と、現在の銀行体系20と、金銭モジュール4、5、6間の取引を仲介するネットワーク（各モジュール及びシステムを接続するラインにより例示したもの）25と、システム20及び安全保障システム21に参加する関連銀行1、2、3と、金銭モジュールの誤動作及びシステムインサイダ（不正）行為を検出するための取引調整システム22と、電子マネーの偽造及び再使用を検出するための金銭発行調整システム23、並びに電子マネーの流通経路を辿るための金融状態システム24からなるものである。

【0049】好ましい実施例において、実行される主要な役割は経済的価値を代行する電子的象徴の発生、ストア、及び移転という3種類の機能を有する金銭モジュールによって実行される。これらは金銭取引モジュール4、金銭出納モジュール5及び金銭発生モジュール6を包含する。これらの金銭モジュール4、5、6は比較的大規模な処理環境の要素となることを意図した不正防止ハードウェア及びアプリケーションソフトウェアの組合せからなることに注目すべきである。

【0050】図2の右上部を参照すると、ここにストアされた電子手形11（図示せず）を収容する金銭取引モジュール4は、電話通信リンク又は近接通信リンクのいずれかによって安全な秘密のプロトコルを用いて外国通貨を交換したり、別の金銭取引モジュール4による支払を行ったりするのに利用される。電子手形11は交換可能であること、すなわち如何なる所望額にもくぐることができるということを意図し、金銭取引モジュール4間で取引される金額は支払者の金銭取引モジュール4にストアされた金額までの額であり得る。

【0051】支払金として電子手形11を受信した受取人の金銭取引モジュール4は、ここに収容した電子マネーの総額又は何ほどの金額を別の加入者の金銭取引モ

ジュール4に移転するためにも用いられる。受取人は選択的にこの電子マネーを彼の銀行口座に預金することができる。

【0052】金銭取引モジュール4にストアされた電子マネーの値はまた、その電子マネーの何ほどの金額を銀行の金銭出納モジュール5に移転することにより、いずれかの関連銀行（例えば、コルレス銀行2又は発行銀行1）において紙幣として回収されることができ、これによって出納係又は自動出納機械（AMT）が同額の紙幣を返還する。当然のこととして、紙幣は等価の電子マネーと交換しうるということが明らかである。

【0053】よく認識される通り、金銭取引モジュール4は電子手形11による通貨の預金、引出、ローン支払、質問及び交換を発行銀行1又はコルレス銀行2における金銭出納モジュール5を介して直接に、又は電話回線を介して遠隔地の発行銀行1もしくはコルレス銀行2の金銭出納モジュール5に対して行うように配置構成されている（これにより現在の内国銀行体系では受け入れられない取引を提供する）。銀行取引の要求があると、金銭出納モジュール5は加入者の銀行口座並びに銀行体系の電子マネー口座についての取引を仲介する。

【0054】加入者は金銭取引モジュール4を所有し、かつ使用するために銀行口座を維持することを要求されないということに注目すべきである。例えば、加入者は金銭取引モジュール4を収容した自立型コンピュータ装置を入手し、この装置を商人の販売時点情報管理ターミナルなどのように、金銭取引モジュール4を収容した他の装置との間でのオフライン仲間取引においてのみ利用することができる。当然ながら、商人は電子マネーを別の商業組織に移転して、その債務を弁済し、又はその電子マネーをそれ自身の銀行に預金することも可能である。

【0055】好ましい実施例において、原始発行銀行1自体以外の発行銀行1において、預金された電子マネーはその後、決済システム3によって実行される中央決算プロセスを通じて原始発行銀行により清算される。決済手続は決済銀行3（図1）により管理されることが理解されよう。各発行銀行1の金銭出納モジュール5はその銀行に預金されているが、他の発行銀行1から発行されたすべての電子手形11を決済銀行3に送信し、それらの顧客の口座に表示された値を清算する。

【0056】引出、外国通貨への交換、貨幣の電子マネーへの交換、又は電子マネーの更新が行われる場合、図2において金銭発生モジュール6は通貨又は信用手形11（図1）のいずれかとしての経済的価値を有する電子的象徴を発生し、かつデジタル化する。これらは関連銀行の金銭出納モジュール5を通じて電子手形11のバケットとして金銭取引モジュール4に送信される。上述した通り、電子通貨手形11は預金によって支持された銀行券と等価であり、金銭取引モジュール4間において

取引される。

【0057】引出処理の間において、金銭出納モジュール5及び金銭取引モジュール4はそのモジュール5からモジュール4への手形11の安全な移転のために、秘密のプロトコルを用いた通信リンクを確立することができる。

【0058】金銭発生モジュール6により発生され、かつ搬送される手形11のレコードは統計的機能及びハウスキーピング機能を維持するため、地方銀行の取引調整システム22及び発行銀行1の金銭発行調整システム23に送られる。決済銀行3において清算される電子手形11のレコードはまた、金銭発行調整システム23に供給される。これらの編集によりシステムの金融状態が金融状態システム24により確認される。

【0059】不一致及び誤動作は安全システム21に報告され、このシステムはシステム中のすべての金銭モジュールに対し、問題がある金銭モジュールのリストを、それらがネットワーク25に接続されたとき、公開（ダウンロード）する。このリストを搬送することにより、金銭取引モジュール4は問題の他の金銭取引モジュール4との取引を禁止される。

【0060】以上において好ましい実施例の全貌が概括されたので、次に個々の要素及びそれらの要素間の処理のより詳細な説明を行うこととする。

【0061】金銭モジュール

図3は金銭モジュールを収容する外部システム又は装置の幾つかの具体例を提示するものである。

【0062】好ましい実施例において、外部システム又は装置は、典型的にデータディスプレイ手段、データ入力手段、データ処理手段、記憶ストレージ手段、直接接触又は無接触双方向通信手段、及び不正行為防止用ハウジングに収納された金銭モジュールを含むものであり、これらのすべては周知の適当な情報伝達手段により相互接続されている。

【0063】金銭モジュールは比較的大きい処理環境のモジュラ要素として具体化され、前述したものと同様の機能を実行するものであることがよく理解されよう。例えば、金銭取引モジュール4は“ヒューレット・パッカ― 95LX”（商品名）などのような携帯用パーソナルコンピュータ装置に内蔵された共同プロセッサとして、又はネットワークに接続されたメインフレームコンピュータ、ワークステーション、販売時点情報管理ターミナル又は電話装置（固定式又は携帯用）における共同プロセッサとして作動することができる。

【0064】金銭出納モジュール5は銀行の金融コンピュータシステムにおける共同プロセッサとして具体化され得る。金銭発生モジュール6は銀行にネットワーク接続された分離処理装置、汎用コンピュータにおける共同プロセッサ、又はそれがより大きいプロセッサにおいて発行銀行1の金銭出納モジュール5と結合されたものと

して構成され得る。

【0065】金銭モジュールは個々に分離した処理装置において装置化されるであろうことが予想されるため、対応するインターフェース回路はホスト処理装置において装備され、これによってその処理装置と金銭モジュールとの間の通信を提供するものとする。

【0066】注目すべきは、本発明に含まれるすべてのクラスの金銭モジュールはプログラマ的に具体化されるか、又は一般的な集積回路を通じて直接的に電気接続されることにより具体化され、あるいは本発明の技術的思想から逸脱することなく以下に述べる機能を提供するために周知の方法を用いて両者を結合することにより具体化されるということである。ここに提示する本発明の技術的思想から判断して、一般的な半導体集積回路技術は、本発明の範囲内において金銭モジュールの機能を実現するための種々の代替物を示唆するものであるということとは当業者にとって自明であろう。

【0067】金銭取引モジュール

一実施例において、金銭取引モジュール4はE-M取引利用には制限されない種々の機能を提供するための汎用コンピュータ、又はワークステーションとして機能する適当な大きさのコンピュータに内蔵されることができる。この後者の適用はパーソナルコンピュータ装置間のリアルタイム・オフライン支払用として、又は情報検索、電話呼出などのようなネットワークサービス、あるいは航空券、劇場の入場券等を購入するためのオンライン支払用として用いることができる。

【0068】別の実施例において、金銭取引モジュール4は携帯用パーソナルコンピュータなどのような個々の携帯用集積回路装置に内蔵される。すなわち、それはあたかも財布のように容易に個人に所持されることができる。図示の通り、好ましい実施例の装置は、データ入力手段としてキーボード、ペン又はスタイラス、タッチスクリーン又は音声認識回路と、ディスプレイ手段としての英数字LCDドットマトリクスディスプレイと、無接触双方向通信手段としての赤外線トランシーバ、及び電話通信手段としてモデム回路に結合されたRJ-11ジャックを含んでいる。さらに、装置は所有者等のデータを蓄積し、かつ処理するための計算機能を提供する種々の電子処理及びストレージ手段をも含んでいる。

【0069】このような外部装置の特定の設計は本発明の要部ではなく、したがって、前述した機能を達成するために他の適当な技術を用い得ることに留意すべきである。例えば、LCDディスプレイパネルに代えてLEDを用いること、直接接続に代えて無線、赤外線、誘導又は容量性通信方法を採用することができる。

【0070】一般に、加入者によって所持される何らかの金銭取引モジュール4は、その収納物に接触することが困難なように自己収納型不正防止ユニットにおいて具体化され、したがって、何者かがその収納物又は構成要

23

素のいずれかについての不正な検査、偽造又は変造を行うことを防止するであろうことが予想される。例えば、その収納物が検査困難なようにエポキシ等のプラスチック成層体により形成された不正行為防止用パッケージに収納された集積半導体回路は、高度の物理的安全性を提供し、同時に必要な記憶、演算、計時及び他のデータ処理機能を提供するものである。

【0071】しかしながら、本発明は、産業上においてそのような安全保障を提供する種々の周知方法が存在する故に、上述のような特定の不正行為防止手段に限定されるものではない。このような不正行為の防止はそのモジュールの所持者もまた、金銭取引モジュール4の幾つかの内部動作のみしか制御できないようにし、彼がその安全機能に何らかの細工を施して他の関係機関又は個人に対して悪用することを防止するものである。

【0072】各金銭取引モジュール4は特定の加入者に対するそれ自体の関係を確保する方法を有し、これによって他の個人又は機関による使用を制限することができる。周知のような個人認識番号(PIN)法の使用に加えて、金銭取引モジュール4はさらに、指紋読取器、声紋分析器、署名分析器又はその他のいわゆる生物学的測定手段などを装備することにより、権限を有する加入者の物理的特定を行うことができる。

【0073】さらに、金銭取引モジュール4は真の所持者のみが正確に応えられるであろうような質問、例えば、所持者の母親の旧姓、彼又は彼女の好きな色彩などの質問を発して客観的に特定人証明を行うことができる。このような技術は、諸機関のための付加的な安全保障を提供し、さらに、そのような安全保障が加入者のデータをその金銭取引モジュール4の所有者以外のものが調査して用いることを保護するものであるため、権限を有する使用者の利益をよく保護するものである。

【0074】金銭取引モジュール4は種々の物理的特徴を有することができるが、それは好ましい実施例の関連する物理的特徴の上に達成される機能として説明される。

【0075】図4を参照すると、金銭取引モジュール4がブロック図において示されている。特に、金銭取引モジュール4は、(1)このモジュール4をモジュールデータ処理手段、入/出力手段(人間が介在する)及び外部装置の通信回路に接続する外部インターフェース30と、(2)取引期間(セッション)を制御及び委託(すなわち、終了させる)し、もしくは無効にする期間管理手段31と、(3)アプリケーション機能を管理するための取引手段32、及び(4)金銭の電子的象徴を収容し、かつ管理する金銭ホルダ38、を有する。

【0076】本発明によれば、その好ましい実施例において次のアプリケーション機能が具体化される。

【0077】対加入者アプリケーション33は、利用者の個人認識番号(PIN)及び生物学的特徴(例えば、

24

指紋、声紋、その他)であって、金銭取引モジュール4のメモリ中にストアされたものを、金銭取引モジュール4に近づこうとする個人のものと比較する機能を実行する。正当な所有者であることが検証された後、金銭取引モジュール4は作動状態に置かれ、利用者はそのモジュール4の記憶内容に対してアクセスすることが許される。このアプリケーション機能においてはさらに、金銭取引モジュール4に収容された情報について加入者へのメッセージ及び加入者の質問が処理される。

10 【0078】対出納アプリケーション34は、金銭取引モジュール4を金銭出納モジュール5に接続してこのモジュール5による預金、引出、貸付金支払処理、及び銀行質問を開始し、かつ実行させる。

20 【0079】支払/交換アプリケーション35は、金銭取引モジュール4間における電子手形11の送信及び受信を統御し、電子手形11をその金額、デジタル署名等について正確にパッケージするプロセスを管理する。このアプリケーションは電子手形11が認識された妥当なフォーマットにおいて伝達されるようにするものである。これは金銭モジュールが支払及び外国為替取引を行うことを許すアプリケーションであることに留意すべきである。好ましい実施例においては、このアプリケーションがなければ、金銭取引モジュール4は別の金銭取引モジュール4に支払を行うことができない。

30 【0080】TLM(Transaction Log Manager)アプリケーション36は、金銭モジュールによって企てられた取引の完了を記録するログ(log)の管理及び監視を行うものである。電子マネーの各完了された移転毎の、図示のレコードは次の通りである。

(1) 移転の形式(例えば、支払、預金、外国為替取引、その他)、(2) 移転の日付、(3) 移転の金額、(4) 発行銀行1の認識番号、(5) 手形認識番号、(6) 通貨単位、(7) 取引において、及び預金、引出及び貸付金支払のために関与する他の金銭モジュールの認識番号、(8) 銀行口座番号、(9) 銀行認識番号、及び(10) 取引の金額、

40 【0081】好ましい実施例において、金銭モジュールの認識番号はそのモジュールの連続番号とみなされ、変更することはできない。

【0082】加入者はこのTLMアプリケーションにおいて、ストアされた移転の金額、日付、及び形式の履歴などのような幾つかのデータフィールドにアクセスすることができる。証明の満期日についての情報もまた、加入者によってアクセスされ、これにより彼のその金銭モジュールの証明を更新し、もしくは再有効化する必要についての情報を得ることができる。

50 【0083】安全維持アプリケーション37は、一般に了解された既知の金銭モジュールの認識番号リストを管理するものである。特に、これは各金銭モジュールに対

しそれがネットワーク25と通信するとき分配されるリストであり、かつ無価値なもしくは偽造された電子手形11を受け入れた金銭モジュール、又はシステムに対して有害と考えられる行為を行った金銭モジュールのリストであることに留意すべきである。

【0084】金銭モジュール間で期間が確立されると、各金銭モジュールは好ましくない金銭モジュールのリストをチェックし、他方のモジュールが不正な金銭モジュールであるか否かを判断する。もし、他方(相手側)の金銭モジュールの認識番号がリスト中に存在すれば、通信は遮断される。

【0085】このアプリケーションはさらに、金銭モジュールに対して新規の証明を入手し、内部クロックを同期化し、かつ安全な暗号キーの発生を管理するプロセスを提供する。

【0086】手形記録アプリケーション39は、金銭モジュール内にストアされた電子手形11の位置認識表及び価値を追跡する機能を実行する。手形11が電子通貨手形であるか、又は電子信用手形であるかということは電子マネーの基本事項である。それは経済的価値を表す電子的象徴であり、その構成ビットは移転に際してデジタル署名され、かつ暗号化された金額、満期日、手形認識表などのような情報を含んでいる。電子通貨手形11及び電子信用手形11は手形記録アプリケーション39により定位置に記録される。

【0087】手形記録アプリケーション39は、各移転後の通貨単位による電子手形11(通貨及び信用の双方)の最新の金額の合計を更新する。満期日、手形認識番号及び発行銀行の認識番号もまた、各手形11の位置において記録される。

【0088】要約すれば、手形記録アプリケーション39は、金銭取引モジュール4にストアされた手形認識番号、発行銀行1の認識番号、手形11の満期日、手形11の記憶位置、及び各通貨単位毎にストアされた手形11の最新の合計金額を追跡する。これらのレコードは電子通貨及び電子信用の双方について維持される。信用手形11、貸付限度額の口座番号が維持される。

【0089】手形アプリケーション40は、電子手形11自体の電子的象徴のストレージを管理する。このアプリケーションはまた、手形11が移転されるべきときに移転を生ずるものである。

【0090】パケット管理アプリケーション41は、別の金銭モジュールに移転されるべき電子手形11のパケットの構成及びフォーマット化を管理する。例えば、パケット管理アプリケーション41は最少数の電子手形11が最先の日付の電子手形11を最初に用いることにより、要求金額の移転を満たすべく用いられるようなアルゴリズムを利用する。選択的に、手形11のパケットが受け取り金銭モジュールに転送されると、パケット管理アプリケーション41はパケットを切離し、日付を検

証し、かつ異なった電子手形11を表すデータフィールドを分離する。

【0091】フォーマット化されたパケットは電子手形11がアSEMBLされるとき、それに付随した幾つかのデータフィールドを獲得する。認識用データフィールドはパケットとしてそれを識別するための表徴を提供する。さらに、手形11の合計値、手形11の数及び手形11の個々の位置のためのデータフィールドが提供される。

【0092】検証アプリケーション42は、受信されたパケットが受取側金銭モジュールがそれらを受け入れるまでに妥当な電子手形11を収容しているか否かを検証する。この検証アプリケーション42はさらに、受け取られた合計額が移転されるべき電子手形11の合計に等しいか否かをチェックする。もし、合計額及び個々の電子手形11が有効であれば、移転の完了を許すために承認票が返送される。さもなければ、“無効”メッセージが送られ、移転は取り辞めになる。

【0093】サービスアプリケーションは、次の2つの範疇に、すなわちクロック/タイマアプリケーション43及び暗号アプリケーションの2つに分けられる。クロック/タイマアプリケーション43は、メッセージの送信と応答メッセージの返信との間の時間などの処理時間切れを制御するための出力パルスを提供する。

【0094】了解される通り、2つの金銭モジュールが通信中であるとき、それらは時間切れプロトコルを監視することができる。例えば、第一の金銭モジュールが第二の金銭モジュールにメッセージを送った後、前記第一の金銭モジュール(“A”)の期間管理手段31は処理手段32が応答を求めている場合にそれに回答するため、タイマをセットすることができる。期間管理手段31はさらに、送信されたメッセージに番号を付す。この番号は第二の金銭モジュール(“B”)の期間管理手段31からの応答メッセージにおいて出現する。

【0095】タイマがメッセージの受信までに終了すると、期間管理手段A31は期間管理手段B31に対し取引がBにおいてなお実行中であるか否かを判定するように質問を発する。Bが応答しなければ、ここで期間管理手段A31は取引を取り辞める。逆に、取引が進行中であるという応答が受信されると、タイマは安全な時間にリセットされる。AがBに対し、初期メッセージに対する応答が受信されなかった回数を所定数まで質問した後、Aは取引を取り辞めることができる。

【0096】このアプリケーションはさらに、個別的に最新の日時を維持するが、これは産業上一般的に用いられている他の一般クロック機能と併せて、受信されるべき電子手形11が満了していないことを検証し、かつ利用者のディスプレイに供するためのものである。

【0097】暗号表記アプリケーションは、パブリックキー44のオペレーション、対称キー45のオペレーシ

ョン及び乱数発生器46を含んでいる。金銭取引モジュール4及びその要素の不正行為防止機能は、人がその装置の構造又は内容を変更するのを困難にするものであるが、周知の暗号作成技術もまた、金銭モジュール間における安全な通信及び支払移転を保証するために採用される。

【0098】当業界において、周知のパブリックキー暗号表記アプリケーション44は、いわゆるデジタル署名又は単に署名と略称されるパブリックキーによるデジタル署名入力を提供するために用いられる。電子手形11におけるデータはデジタル数により表現される。電子手形11はこの数から形成されるデジタル署名により署名効果を認める。ここで、デジタル署名は対応するパブリックキーを知悉したいずれかの者による特定のメッセージに対応するものとしてチェックされる。この“いずれかの者”とは、好ましい実施例においてはすべての他の金銭モジュールである。

【0099】このアプリケーションは各金銭モジュールに対し、デジタル署名の信憑性をチェックする能力を付与するものである。デジタル署名された電子手形11を受信した金銭モジュールは他者に対してさらに署名及び転送を行い、この他者はまた、それをチェックし、署名し、かつ分配するものである。

【0100】パブリックキーによるデジタル署名の片道性又は非可逆性、及び演算の複雑性に基つき、妥当な時間内にそれらを解読し、かつ複製することは困難であるため、偽造を防止した安全システムが形成されるものと考えられる。

【0101】最後に、このアプリケーションは必要に応じて安全なパブリックキー及びプライベートキーを発生

【0102】対称キー暗号アプリケーション45は、金銭モジュール間の個々の取引期間の安全性及びプライバシー保護のためにこの業界では周知のプライベートキーアルゴリズムを提供する。好ましい実施例において、このアプリケーションは2つの金銭モジュール間の為替取引中における情報を保護するための暗号化／解読手段を提供する。

【0103】ナショナルデータエンクリプションスタンダード(DES)システムなどとして知られた周知の対称キー暗号表記技術、又は他の適当な暗号表記技術はこのアプリケーションにおいて適用される。例えば、暗号技術により保護された通信に対する関心の高まりに基つき、製造者はデータの暗号化及び解読を実行する種々の半導体集積回路装置を開発している。例えば、サイリンクコーポレーションのCIDEデータ暗号表記装置は、本発明においてこのアプリケーションにふさわしい形で入力可能な暗号表記／解読回路装置である。DESアルゴリズムの連邦(アメリカ合衆国)命令による使用に基つき、これらの装置はそのアルゴリズムの具体化に

において広く用いられている。

【0104】金銭モジュールによって使用される特定の暗号法の詳細は本発明の要部ではなく、したがって、それは特定の暗号表記技術に限定されるものではない。

【0105】乱数発生アプリケーション46は、対称キーアプリケーション45のための新たなプライベートキー、及びパブリックキーアプリケーション44のための新たなパブリック／プライベートキーを発生するための同様な乱数を発生する。このアプリケーションは予知できない方法において、仮期間キーを変更するために用いられる。

【0106】このような乱数発生能力を提供する回路はこの分野においては周知である。例えば、“ノイジー”ダイオードを利用する回路が周知の通り乱数を発生する。乱数はベキ剰余アルゴリズムなどのような数学的アルゴリズムを具体化することによりシード数から明白な乱数を発生する疑似乱数発生回路によっても提供される。クロック又はカウンタの使用はよく用いられる別のランダムデータ源を提供する。よく理解される通り、乱数発生アプリケーション46は仮の数を発生するために当業者にとって周知の技術を用いることができる。

【0107】前述した機能は周知のプログラミング技術及び／又はハードウェアによって、及びある種の場合にはその各々のリソースの結合によって達成される。当業者によって認識される通り、これは本発明の金銭モジュールの基本的特徴を逸脱することなく、特定のアプリケーション要求において自在に種々の変更を加えることができる。

【0108】金銭出納モジュール

発行銀行1及びコルレス銀行2の双方における銀行体系20は金銭出納モジュール5を通じて本発明のシステムに接続される。金銭出納モジュール5は何らかの汎用コンピュータ又はワークステーションに内蔵される。金銭出納モジュール5の特定の設計は、金銭取引モジュール4と同様、周知のプログラミング技術又はこれに充てられるコンピュータハードウェア、あるいはその組合せにおいて容易に具体化される。当業者によってよく認識される通り、金銭出納モジュール5の種々の設計は、ここに述べる諸機能を具体化するために採用される。

【0109】金銭出納モジュール5の一実施例の詳細は図5におけるブロック線図で示されている。このモジュール5は前述した金銭取引モジュール4と同一の多くの要素及びアプリケーション機能を含んでいる。したがって、同一の要素については略記するに止め、ここでは固有の要素について詳述することにする。金銭出納モジュール5はシステムの他の金銭モジュールと同様、必要な安全性確保のため、この分野において共通する形式の不正行為防止構造内に収納される。

【0110】金銭出納モジュール5は外部インターフェース30、期間管理手段31、取引手段32及び金銭ホ

ルダ38を含み、これらは前述した金銭取引モジュール4における対応要素と同様の機能を実行する。

【0111】略述すれば、外部インターフェース30は金銭出納モジュール5をこのモジュール5のホストプロセッサ内における他の処理及び通信手段に接続する。また、期間管理手段31はこの金銭出納モジュール5と別の金銭モジュールとの間の取引期間を制御し、かつ委託（終了させる）、又は取り辞める動作を行う。また、金銭ホルダ38は電子マネーのストア及び検索を管理し、さらに、取引手段32は出納アプリケーション34、TLM32アプリケーション36、安全維持アプリケーション37、対銀行アプリケーション47、対金銭発生アプリケーション48及び対取引アプリケーション49の機能を管理するものである。

【0112】次のリストは金銭取引モジュール4において見出されるアプリケーションと機能上同一の金銭出納モジュール5におけるアプリケーションを略述するものである。

- 対出納アプリケーション34：預金及び引出機能を別の金銭モジュール5に接続する。
- TLM32アプリケーション36：取引の詳細を記録するために取引ログ管理を行う。
- 安全維持アプリケーション37：互いに折合った金銭モジュールのリストを管理し、証明を加え、クロックを同期化し、さらに、安全なデジタルキーの形成を管理する。
- 手形記録アプリケーション39：通貨単位による手形11の位置、値及び認識番号の軌跡を辿る。
- 手形アプリケーション40：電子手形11のための為替ストレージを管理し、かつ手形11についての移転を発生する。
- パケット管理アプリケーション41：異なった金銭モジュールに移転されるべきパケットの組立及び分解を管理する。
- 検証アプリケーション42：受信されたパケットが有効な電子手形11を含んでいることを検証する。
- クロック/タイムアプリケーション43：取引の時間切れ、電子手形11の効力の消滅、証明の効力消滅、及び一般的クロック機能を制御する。
- 暗号表記

(i) パブリックキー44：手形11に署名し、かつ有効化する署名機能及び取引安全期間を設定するために用いられる。

(ii) 対称キー45：取引期間の安全性を制御する。

(iii) 乱数発生アプリケーション46：安全な暗号キーのための疑似乱数を発生する。

【0113】幾つかの顕著なアプリケーションは、対銀行アプリケーション47及び対取引アプリケーション49である。対銀行アプリケーション47は金銭出納モジュール5が銀行のオンラインシステムにより質問及び口

座登録するためのデータ交換を実行できるようにするインターフェース手段を提供する。このアプリケーションは顧客の口座番号を、要求されている取引の口座及び形式と相互チェックするためにも用いられる。

【0114】対取引アプリケーション49は、預金、引出及び貸付金支払を実行する。このアプリケーションは金銭出納モジュールが加入者の金銭取引モジュール4と取引している限り作動するものである。

【0115】上述した通り、金銭出納モジュール5は発行銀行1又はコルレス銀行2と関連する。金銭出納モジュール5がコルレス銀行2と関連するとき、それは金銭取引モジュール4、コルレス銀行2のオンラインシステム、及び発行銀行1における金銭出納モジュール5間の預金、引出、及び貸付勘定への支払を仲介するために用いられる。

【0116】金銭出納モジュール5は発行銀行1モードにおいて作動するとき、他の金銭モジュール及び発行銀行1のオンラインシステムとの間での預金、引出及び貸付勘定への支払を仲介するために用いる。さらに、金銭出納モジュール5が発行銀行1モードにおいて作動するとき、対金銭発生アプリケーションは新たな手形11を要求するときに採用される。

【0117】基本的に、対金銭発生アプリケーション48は電子手形11を要求する銀行機能を実行する。それは発行銀行1の金銭出納モジュール5を金銭発生モジュール6に接続する。

【0118】発行銀行1の金銭出納モジュール5において達成される他のすべての要素は、前述した同様の名称の要素及びアプリケーション機能と基本的に同一である。

【0119】金銭発生モジュール

図6は金銭発生モジュール6のアプリケーション機能を示すブロック線図である。金銭発生モジュール6は発行銀行1が電子マネーを発行するために利用するメカニズムを提供する。金銭発生モジュール6もまた、他の金銭モジュールについて前述したと同様の安全保障上の理由により不正行為防止用パッケージ内に収納される。

【0120】金銭発行モジュール6は電子マネーを（後に詳述する電子手形11の形態において）発生し、かつそれらが発行銀行1の金銭出納モジュール5を通じて他の金銭モジュールに分配するものである。金銭発生モジュール6は電子マネーに対する要求に応じるため、他の金銭モジュールには存在しない新規のアプリケーションを含んでいる。これは金銭発生アプリケーション50である。

【0121】金銭発生アプリケーション50は、必要な預金によって支持された通貨又は信用認可のいずれかである経済的価値を表した電子的象徴を発生し、かつフォーマット化するとともに、そのシークレットキーに関連するパブリックキー暗号を用いてこれらの電子手形11

31

にデジタル的に署名し、これによって発行銀行の金銭出納モジュール5に送られるようにするものである。

【0122】金銭発生モジュール6において対銀行アプリケーション47は、銀行体系の何らかの不規則性を警告し、取引調整システム22に対して取引ログにおける取引記録を付与（オフロード）し、さらに、金銭発行調整システム23に電子手形11を転送するというように注目すべきである。金銭発生モジュール6の他のすべてのアプリケーションは前述した金銭モジュールの同一名称のアプリケーションと同じである。

【0123】ネットワーク

本発明の一実施例によれば、その個々の要素は図7に示すようなネットワーク25において通信を行うことができる。ネットワーク25は発行銀行1、コルレス銀行2、決済銀行3及び証明機関28を互いにリンク接続するものである。

【0124】金銭取引モジュール4は電話交換、又は銀行内における特定のターミナル設備（例えば、ATMブースにおける付加的な無接触又はケーブルによる接続）を介してネットワーク25に結合される。1つの通信階層は取引要求（例えば、預金、引出等）、手形11のパケット及び新たな証明を、ネットワーク25を通じて確実に搬送する。好ましい実施例において、ネットワーク25は金融サービスのディレクトリ（登録簿）誘導を提供し、かつすべての金銭モジュールについての好ましくない金銭モジュールリスト及び金銭モジュールクロックを更新する。

【0125】よく理解される通り、ネットワーク25は例えば、電話回線、光ファイバ地上ライン及び人工衛星を用いてデジタル情報に対するアクセスを許容し、かつ送信するための接続、タイミング及び制御用ソフトウェアを含む周知のデータリンク又は通信システム及び技術を用いることができる。ネットワーク25は商業的に入手可能なプロトコル及びオペレーション技術として、例えば開放システム相互接続ネットワーク標準として、国際標準化機構（ISO）によって規定されたものを用いることができる。ネットワーク25の特定の設計は本発明の要部ではなく、前述したデータ通信機能を達成するためには他の適当な技術を用いることができることに留意すべきである。

【0126】各実体（銀行1及び2、証明機関28、又は決済銀行3）はまた、個々のローカルネットワーク16、17、18及びそれらを大規模ネットワーク25に導くゲート通路を有するものとする。大規模ネットワーク25はメッセージを適当なローカルネットワーク16、17、18に接続すべく道筋を決定するディレクトリサービスを提供する。ローカルネットワーク16、17、18は適当な金銭モジュール又は安全保障手段27へのメッセージの道筋を決定する応答能力を有する。安全保障手段27は各関連銀行及び証明機関28に関連

32

し、システムの安全性を具体化するために用いられる。

【0127】図7はネットワーク25の好ましい実施例を図解したものであり、概していずれかの関連銀行の金銭モジュールが他の銀行及び金融機関の金銭モジュールに結合されること、又は別の加入者の金銭取引モジュール4が通信リンクを介してスイッチング及び処理センタに直結され、及び選択的に各実体におけるローカルネットワーク16、17、18に接続されることを示している。

10 【0128】金銭モジュールは最大量のメッセージの送信を行うため、ローカルネットワーク16、17、18の決定構造（典型的には、バンク・サブネットワーク）を識別することのみが必要である。ローカルネットワーク16、17、18は期間を確立するために適当な金銭モジュールにメッセージを導く。期間が確立されると、ネットワーク25はすべてのメッセージを2つの金銭モジュール間において誘導する。ネットワーク25はさらに、金銭モジュール及び安全保障手段27間でメッセージを制御する。

20 【0129】金銭取引モジュール4は預金、引出、貸付勘定への支払、更新又は質問のためにネットワーク25を通じて通信を行うことができる。出納モジュール5及び金銭発生モジュール6はネットワーク25に周期的に信号を送って安全保障情報を更新する。“サインオン”（ネットワーク接続）は金銭モジュール期間管理手段31によって開始されるか、又は再証明が要求され、もしくはは好ましくない金銭モジュールリストに変更が生じた場合には、銀行安全保障手段27により開始される。

30 【0130】銀行サービスのディレクトリは、基本的には電子手形11を更新し、及び外国為替取引を行うために金銭モジュールに受け入れられる。いずれかのサービスのための関連銀行のリストはネットワーク25から入手される。

40 【0131】好ましい実施例において、ネットワーク25は本発明の個々の要素に対するタイムサービスを提供する。取引モジュール4、出納モジュール5及び金銭発生モジュール6と安全保障手段27のクロックはネットワーク25におけるネットワークサーバ26により各金銭モジュールがネットワーク25にアクセスするたび毎に更新される。

【0132】ネットワークサーバ26はローカルネットワーク16、17、18に対するゲート通路サービス、及び後述の金銭モジュールサービスを提供する。ネットワークサーバ26の好ましい実施例におけるアプリケーション機能は図8のブロック線図に示されている。次のアプリケーション機能はネットワークサーバ26について規格されたものである。

（1） 外部インターフェース56 - ネットワーク25に接続される通信階層、及び（2） 通信期間管理アプリケーション57 - 金銭モジュール間及び金銭モジュール

33

ルと安全保障手段27との間の通信期間を管理する。

【0133】アプリケーションサービスは次のようにして提供される。

(3) ネットワークサインオン管理アプリケーション58-金銭モジュールネットワークのサインオンプロセスを制御する、(4) 同期化日時アプリケーション59-システム時間に同期化された金銭モジュールクロック/タイマ43のサービスを維持する、(5) ルートメッセージアプリケーション60-メッセージの道筋を決定し、サインオンの間及び金銭モジュール期間におけるメッセージ誘導の制御を行う誘導サービスであり、さらに、(6) 銀行への指示サービス61-関連銀行により提供されるサービスの情報を提供する。

【0134】当業者によって認識される通り、周知のスイッチングセンタ及び処理センタを、金融機関と、同じセンタに結合された他のものとの間におけるネットワーク並行動作のために用いることができる。

【0135】電子手形

ここで電子手形11自体の構成要素について詳細に説明する。

【0136】経済的価値を代行する電子通貨手形11は、基本的には発行銀行1における営業性預金により支持された取引要求(預金、又は引出)から生ずる電子的象徴である。種々の時間及びシステムの種々の点において、これらの手形は電氣的又は磁氣的形態において、あるいは電磁波として発現する。これらの手形11は紙幣と同様に幾つかの取引を通じて移転されることができ、各手形の価値に等しいか、又はそれ以下の金額において換金もしくは移転できる交換可能性という付加的な財産的価値を有する。

【0137】複数の手形11は、その手形11への移転記録を添えるとともに、それを移転する金銭モジュールのプライベート暗号キーを用いて署名することにより分割される。しかしながら、電子信用手形11は好ましい実施例においては、1回限りしか移転できない。これはその受取人が貸付を実現するように信用手形11を預けなければならないからである。

【0138】信用手形11は通貨手形11とは異なり、加入者の貸付勘定において振り出される。各信用手形11はそれが振り出された口座番号を支持している。この口座はその手形11が振り出された回転信用又は貸付限度であり、今日の銀行産業において、小切手又はクレジットカード勘定が機能する方法と同様に働くものである。信用手形11は口座の貸付限度の一部又は全部を代表することができる。

【0139】好ましい実施例において、信用手形11は口座の所有者によってのみ別の金銭取引モジュール4に移転され、信用手形11の受取人はそれを彼の口座中に通貨として預金することのみが可能である。これにより、信用手形11は決済銀行3において通貨により決済

34

される。加入者の銀行は決済された信用手形11の受領時において貸付を認識する。

【0140】信用手形11が回収されると、好ましい実施例において、それらは如何なる会計取引をも開始させるものではない。最新の貸付限度処理は、加入者の金銭取引モジュール4における貸付限度の金額に追従するように変更される。加入者が貸付限度を維持する発行銀行1と通信するときは、金銭取引モジュール4における貸付限度の総額は銀行体系20における貸付限度に対する何らかの調整に基づいて除去及び置換される。しかしながら、全信用手形11に未済貸付金を加えたものは貸出限度の総額以下でなければならない。

【0141】電子手形11はデータフィールドの3つの集まり、いわゆる本体グループと、移転グループ、並びに署名及び証明グループからなっている。データフィールド本体グループは次の情報を含んでいる。

(1) 電子手形11の型、すなわち通貨手形11、及び信用手形11のいずれであるか、(2) 発行銀行1の認識番号、(3) 通貨単位の認識番号、(4) 手形認識番号、(5) その発行日、(6) その満期日、(7) 加入者の口座番号(信用手形11のためにのみ用いられる)、(8) 手形11の金額、及び(9) 金銭発生モジュール6の認識番号、である。

【0142】データフィールドの移転グループは次のものを含んでいる。

(1) 電子手形11が移転された回数の合計(通貨手形11の場合のみ適用される)、(2) 割り当てられた手形11の振出元に、移転日、移転額、及び受取人の認識番号を示す移転レコードのリスト。

【0143】データフィールドの署名及び証明グループは次のものを含んでいる。

(1) 金銭発生モジュール6のデジタル署名、(2) 金銭発生モジュール6の証明、(3) 各支払人の署名及び証明を含む支払人リスト、(4) 支払人のデジタル署名、及び(5) 支払人の金銭モジュールの証明。

【0144】手形11の移転レコードと、移転された一連の支払の署名及び証明は、送られた電子手形11を構成し、手形11の残額はそれがストアされた金銭モジュールの手形ディレクトリ39に記録される。

【0145】電子手形11の信頼性は金銭発生モジュール6のデジタル署名の有効性、及び過去の支払人(もし、存在するならば)の署名の有効性によって判断される。この情報に何らかの不一致があると、如何なる電子手形11の移転も取り辞めになる。

【0146】安全性の尺度として、手形11はその満期日までの限られた時間だけ効力を認められる。満了した手形11は移転できず、それは参加銀行との取引によって更新されなければならない。このため、金銭取引モジュール4が金銭出納モジュール5と何らかの取引を行う

限り、金銭取引モジュール4にストアされたすべての電子手形11は金銭出納モジュール5に移転され、これにより電子手形11はそれらが満了するまでに更新されたものと置換される。この安全保障手続はまた、悪い手形が広く循環することを防止するものである。

【0147】手形11が別の金銭モジュールに移転される限り、デジタル署名された移転レコードであって、それがどこから移転されたものであるかを示すものが付け加えられることは容易に理解されるであろう。したがって、電子手形11の受領者はまた、その手形11の過去のすべての所有者のレコードを受信することになる。

【0148】例えば、50ドルの電子手形11が生成され、これが金銭取引モジュール4によって回収されることができる。それは他の金銭モジュールに10ドル、10ドル、30ドルの額面金額において移転されるものとすれば、受領者の金銭モジュールは手形11を最初金銭取引モジュール4を識別する移転レコードとともに受信する。10ドル手形11の受領者がそのうちの5ドルを第三者に移転すると、この第三者は手形11を先の二人の所有者を示すレコードとともに受信する。この5ドルの手形11がここで預金されるものとすれば、そのレコードはこの実施例の決済及び調整プロセスによってその銀行体系に返還する道を見出し、初期50ドル手形11の他の断片と整合する。

【0149】手形11の預金又はそれを支払に用いることは、移転された手形11の受領者のみが行えることである。金銭モジュール検証アプリケーション42は各移転の署名をチェックして手形11が有効であるか否かを判定するとともに、最終移転者における認識番号が手形11の最新の所有者であることも検証するのに用いられる。これは手形11の新たな所有者が移転されたものより大きい金額として用いることを防止するものである。それはまた、認識番号が一致していないのに手形11を別の金銭モジュールにおいて使用すべくコピーされることを禁止するものである。

【0150】よく認識される通り、加入者は金銭取引モジュール4内にストアされた電子手形11に対するある種の情報にアクセスすることができる。

【0151】特に、加入者はストアされた電子手形11の合計金額、手形11の通貨単位、電子手形11の形式、すなわち通貨であるか、信用であるか、及び各手形11の額面の情報を選択することができる。

【0152】システム安全保障

システムの安全保障は、参加銀行及び証明機関28によって維持される。証明機は金銭モジュールの証明を発行し、かつ分配するものである。金銭モジュールの証明は実際には金銭モジュールの認識番号、そのパブリックキー、その金銭モジュールの認識番号及び証明キー（後述）を用いたパブリックキーのデジタル名及び証明キーの型（バージョン）である。証明はただ一つ特定の

金銭モジュールが関連するという点において独自の方式である。

【0153】証明機関28は、まず金銭モジュール証明プロセスを制御し、次いで、悪い金銭モジュールの認識番号リストを分配することにより金銭モジュール相互の取引に先立ってその取引にかかわる金銭モジュールの有効性を保証する手段を提供する。

【0154】好ましい実施例において、金銭モジュールの証明は最初に証明機関28によりその金銭モジュールにロードされる。証明機関28は証明キー（証明機関28のプライベートキー）を用いて各金銭モジュールについての証明を発行する。それはこの分野において、通常用いられるバージョン制御プロセスにより周期的に変更され、かつ分配される。よく認識される通り、どの金銭モジュールも古いキーによって発生した証明を検証するために幾つかの証明キーバージョンをストアすることとなる。証明が時間切れとなることが予想されるため、少数のバージョンが維持されればよい。

【0155】証明はその発生後の拘られた時間内のみ有効である。証明の効果が満了すると、金銭モジュールは他の金銭モジュールと取引できなくなる。不正に変更されたことが発覚したいずれかの金銭モジュールは、それらの証明が更新されるまでにシステムに及ぼす損害額を制限される。

【0156】不正な金銭モジュールが取引に用いられることを阻止するためには、正当な金銭モジュールがリストの更新後、直ちにその不当な金銭モジュールの最新のリストを受け入れることができるようにするのが望ましい。当然ながら、これは金銭取引モジュール4に対し、最新のリストを得るため、周期的に証明機関28にアクセスすることを要求する。金銭取引モジュール4の取引能力の上に時間的制限を（電子手形11に設定された時間的制限に加えて）置くことは加入者をして周期的にネットワーク25を通じた証明機関28へのアクセスを強制し、これによって新たな証明とともに最新の不当金銭モジュールリストを受信させる。好ましくは、証明の有効期間が安全保障の必要に応じて頻繁に監視され、かつ調整される。

【0157】証明機関28は安全保障手段27（図9参照）を通じてその更新された証明キー及び金銭モジュールの証明をオンラインで分配する。システム安全保障の重要な要素は、参加銀行の安全保障手段27及び証明機関28の安全保障手段27によって提供される。

【0158】ここで図10を参照すると、安全保障手段27の好ましい実施例のブロック線図が示されている。証明機関28又は銀行のローカルネットワーク18における安全保障手段27は次のアプリケーション機能を含んでいる。

(1) 外部インターフェース54 - 銀行のローカルネットワーク18又は証明機関のローカルネットワーク1

7に接続するための通信階層である。

(2) 期間管理手段55・取引期間の安全性を制御する。

(3) 証明発行アプリケーション50・幾つかの金銭モジュールに対する証明を行う。

(4) 口座プロフィール発生アプリケーション51・銀行口座プロフィール(後に詳述する)を証明及び署名し、金銭取引モジュール4が加入者の異なった銀行口座にアクセスすることを許可する。

(5) 証明分配キーアプリケーション52・証明機関28の、金銭モジュールに対する有効パブリックキーのリストを分配する。

(6) 不当金銭モジュール制御アプリケーション53・不当金銭モジュールのリストを制御し、かつ分配する。

(7) サービス・先に述べた金銭モジュールにおける暗号機能44、45、46と同じである。

【0159】証明はやがて時間切れとなるため、金銭モジュールには新たな証明を周期的に適用することが要求される。金銭モジュールは新たな証明を受信するため、新たなパブリックキー及びプライベートキーを発生する。新たなパブリックキー、金銭モジュール認識番号及びその古い証明は古いプライベートキーを用いてデジタル署名された直後において証明機関28に提示される。

【0160】証明機関28は署名をチェックし、それが有効であれば、新たなパブリックキー及び認識番号をサインし、かつその証明を将来の満期日とともに金銭モジュール送信する。証明機関28の安全保障手段27はネットワーク25を介して不当な金銭モジュールのリストを分配する。各参加銀行の安全保障手段27は最初に手形11を保持する金銭モジュールの認識番号、無効性又はそれが偽造されたものであることを報告する。それらの認識番号は安全保障手段27を通じて送信され、証明機関28により編集される。

【0161】このようなすべての認識番号は金銭出納及び発生モジュール5、6それぞれ分配される。金銭モジュールは不当金銭モジュールリストにおいて見出された金銭モジュールとは取引しないであろう。選択的に、安全性に対する際立った違反を示すような金銭モジュールについては、金銭取引モジュール4にも分配される。

【0162】金銭取引モジュール4が紛失又は盗難にあった場合には、加入者はそのことを彼の銀行又は証明機関28に報告し、これによって金銭モジュールの認識番号はそれ以降の如何なる取引をも禁止するために不当な金銭モジュールリスト上に掲載される。

【0163】システムの安全性は金銭モジュールの取引能力を阻止し得ることにより提供されるものであるが、それは金銭モジュールの証明に加えて、電子手形11上に満期日を与えることによっても維持される。

【0164】先に述べた通り、手形11はそれか発生した後の限られた時間内のみ有効となるようにされる。その満了日は必要に応じて監視され、かつ有効化される安全パラメータである。手形11の有効期間は手形11の価値によって変えることができる。好ましくは、大きい手形11は小さいものより短い期間において満了させられる。例えば、100万ドルの手形はその偽造の重大性に鑑み、発生後5日間で満了するようにされるが、50ドル手形11はその発生日から1ヵ月後で満了するように決定される。

【0165】金銭取引モジュール4は満了した手形11を受付けないが、それは満了した手形11を預金し、又は交換すること、もしくは新たな手形11のためにそのまま維持されることができる。満期日は何らかの電子手形11が移転されるまでに金銭モジュールにおいて検証アプリケーション42及びクロック/タイマアプリケーション43によってチェックされる。個別的に金銭モジュールがパワーをなくしたときは、そのパワーが復活した後、モジュールが再びネットワーク25とつながり、その安全パラメータが更新されるまでは手形11の支払又は交換を行うことができない。

【0166】上述した通り、加入者は典型的にすでに証明を受けた金銭取引モジュール4を入手することができる。加入者に対して金銭取引モジュール4自体を付与することは新規のPIN、生物学的又は他の個人的秘密情報をそれに割り当てることにより達せられる。

【0167】金銭モジュール4の何らかの個人化が処理される前に、金銭取引モジュール4は出納アプリケーション34にすでにストアされた銀行口座があるか否か、又は手形アプリケーション40が幾つかの電子手形11を含んでいるか否かをチェックする。これらのいずれの場合においても、金銭取引モジュール4は加入者がそのモジュールに新たな秘密情報を付与することを禁止するであろう。

【0168】もし、金銭取引モジュール4が口座番号もしくはストアされた手形11を有しない場合、加入者は、金銭取引モジュール4により再び検証されるPINを入力するか、又は金銭取引モジュール4が加入者の固体的特徴を学習するプロセスを実行することにより、その加入者がその口座番号等を確保することができる。個人化が完了すると、金銭取引モジュール4をアクセスする加入者は金銭取引モジュール4に秘密情報を提示するサインオンが有効に完結することを要求する。加入者が金銭取引モジュール4にサインオンできるならば、彼はPINを変更し、又は固体的特徴を再導入することができる。

【0169】加入者が彼のPINを失念するか、又は彼の固体的特徴の読取に影響を及ぼす事態が生じた場合、加入者は彼の金銭取引モジュール4を関連銀行にもっていくことができる。そこで、所有する口座中に何らかの

電子手形11を預金し、かつストアされた銀行口座番号を破棄するような特別の取引が実行され得る。加入者はここで新たな秘密サインオン番号及び特徴を登録することができる。取り除かれた電子手形11は金銭取引モジュール4に返還され、銀行口座番号が更新される(後述の銀行アクセス参照)。

【0170】加入者は彼が金銭取引モジュール4の所有者になれば、システムに彼自身を識別させるということは要求されない。金銭モジュールの特定は取引毎に行われるものであるが、金銭取引モジュール4の所有者は秘密にして置くことができる。もし、その関係が露見すると、何者かはその関係が強固に成立している期間だけは加入者の全取引を追視することができる。加入者が彼の認識番号を明らかにしなければならない唯一の時間は、彼がその金銭モジュールを銀行口座に関連させるか、又は失った金銭を取り戻そうと望むときである。

【0171】加入者が支払及び外国為替についてのみ金銭取引モジュール4を使用することを選択すれば、彼はその秘密関係を維持することができる。加入者は複数の金銭取引モジュール4を取得すること、そして、例えばその1つを銀行口座に関連接続し、残りのものを匿名の支払のために維持できることが理解されよう。他の金銭取引モジュール4は他の金銭モジュールとの交換、又は現金を電子手形11と交換することにより、手形11をロードすることができる。

【0172】金銭モジュール価値の交換

金銭取引モジュール4が機能しないか、又は紛失もしくは盗難にあった場合、加入者はその事態が発生したときにおける金銭モジュールのストア値を取り戻すことが可能である。これは損失金銭の請求を行おうとする限り、加入者がその金銭モジュールに対する匿名性の選択を放棄することを要求し、彼がその金銭取引モジュール4の所有者であることを証明しなければならない。

【0173】電子手形11の交換を行うため、加入者はまず彼の金銭取引モジュール4を銀行口座に関連付けるか、又は金銭取引モジュール4の所有者であることを証明機関28によって登録することができる。電子手形11の移転に伴う取引が行われるたびに、加入者はホストコンピュータ支配から移転可能な廉価な不揮発性(持久)ストレージに対し、相手側の金銭モジュールの認識番号及び手形認識番号を特定する取引ログを節約することができる。このログは加入者が価値交換を要求するときに提示される。このログは次に損失電子マネーの真の値を判定するために調整ファイルと比較される。

【0174】この手続に対する変形例は、金銭取引モジュール4内における金銭をしばしば更新することである。これは金銭取引モジュール4中の手形11が発行銀行1において取引レコードにより代表されることを意味する。手形11の存在は、これらのファイルを走査することにより検証することができる。

【0175】第三の変形例は、システムが金銭の更新中において金銭モジュールの取引ログを捕捉できるようにするものである。これらのレコードは複写され、かつそれらの取引履歴を記憶するために発行銀行1に送られる。手形11の存在は先の変形例と同様に検証される。

【0176】銀行アクセス

本発明の一局面によれば、顧客の金銭取引モジュール4は預金、引出、移転、その他をシステムに参加したいいずれかの銀行において行うために彼の口座をアクセスすることができる。例えば、典型的な加入者は参加銀行の1つにおいて、普通預金口座及び当座預金口座を有することが可能であるが、その一方で遠隔地の金融機関においていわゆる金融市況勘定、そして多分第三の参加銀行における貸出限度勘定を維持することができる。加入者の金銭取引モジュール4はネットワーク25を介してアクセスされるいずれかの銀行又は金融機関において、預金、引出、貸付金支払及び質問を行うため、彼の口座にアクセスすることができる。

【0177】加入者が複数の口座を有する場合、その加入者の口座と銀行との関係は、金銭取引モジュール4の対出納アプリケーション34における口座プロフィール中にストアされる。複数の口座は個々の加入者の関連する個人口座番号“PAN”により互いに関連接続される。

【0178】口座プロフィールは支店における銀行加入者サービス代行業務の制御下、又は特定の対話を利用する電話通信を通じて個々に発生する。例えば、加入者は彼のPAN及びPINにより彼自身の状態を認識することができる。彼は彼の金銭取引モジュール4から、アクセスすることを望む各口座番号を登録することができる。これらの口座番号は銀行の口座参照ファイルにおいて検証される。金銭取引モジュール4に対する口座の相互参照は、彼らがそのように選択した場合において各銀行に維持される。

【0179】典型的な口座プロフィールの構成は次の通りである。

- (1) 銀行認識番号：各銀行毎に1つ、(2) 口座番号、(3) 口座形式…例えば、当座、普通、信用、(4) 口座リスト上の安全保障手段27の署名。

【0180】口座番号のリストは銀行安全保障手段27によりデジタルサインされるものであることが理解されよう。さらなる安全保障として、口座プロフィールは周期的に更新されたパブリックキーにより再署名される。アクセスの基本的安全性は銀行の安全保障手段27のデジタル署名により提供される。

【0181】銀行体系(銀行会計アーキテクチャ)

好ましい実施例の顕著な特徴として、システムの方法は今日行われている会計方法とその変形例を並行して実施することができる。好ましい実施例のシステムは、種々の銀行において現実に行われている会計方法の種々の形

10

20

30

40

50

41

式を踏襲するものである。しかしながら、本発明の好ましい実施例においては、現在の銀行体系とは異なり、経済的価値を要求に応じて発生するということが重要である。したがって、そこには現金又は小切手の明細(inventory)は存在しない。営業性預金から得られた電子通貨及び電子クレジットはリアルタイムで発生する。電子為替媒体を用いることによるこのような紙上明細の排除は、必要なリアルタイム会計を提供するために一般的に実施されている会計技術にある種の補充を要求する。

【0182】したがって、本発明の実施例は現在の銀行体系20において用いられているものに補充するための会計構造を提供する。改良された銀行会計方式は、金銭取引モジュール4と金銭出納モジュール5との間における金融取引が生じた場合、又は決済銀行3が何らかの清算手続を実行する場合において、電子マネー及び各銀行の責務を監視するのに用いられる。

【0183】電子手形11が金銭出納モジュール5に対して授受されると、多くの場合、銀行体系20のレコードに影響する会計取引が発生する。逆に、金銭取引モジュール4間の移転は如何なる形式的な会計手続を伴わず、それらは電子手形11の移転のみを伴うものである。

【0184】説明中のシステムにおいて、各通貨単位の下で分類される銀行の各形式について利用されるために、次のような勘定の取決めが存在する。発行銀行1において、

(1) 金銭発行勘定：発行されたが、清算されていない金銭を反映する負債勘定、

(2) 金銭借入勘定(due account)：銀*30

銀行の形式	口座名	形式	所有者	略号
発行	金銭発行	負債	発行	MI
	借入	資産	発行	MD
	決済銀行預金	資産	発行	DC
	コルレス銀行マネー	負債	コルレス先	CM
	通過金銭	負債	発行	IT
コルレス	外国為替	負債	発行	FX
	発行銀行預金	資産	コルレス先	DI
	借入	資産	コルレス先	MD
	通過金銭	負債	コルレス先	IT
	外国為替	負債	コルレス先	FX
決済	清算勘定	負債	発行	CA

【0188】預金からの引出を要求するような取引処理は、妥当な口座が貸方記入及び借方記入されるようにする勘定処理を選択される。この勘定処理は、この分野ではよく知られたソフトウエアプログラム及び方法を用いるものであり、それは前述した会計手続を提供するためにしばしば実施された周知の何らかのプログラム及び方法が本発明における使用にとってふさわしい場合に限り採用される。本発明の会計手続のよりよい理解のため ※50

42

*行口座に預金された金銭を反映する資産勘定、

(3) 決済銀行預金勘定：決済銀行3における清算勘定を反映する資産勘定、

(4) コルレス銀行の金銭勘定：電子マネーを分配するためにコルレス銀行2によって引き出されるその銀行2によって所有される不正勘定、

(5) 通過金銭勘定(money in transit account)：各銀行によって所有される残高なし負債勘定であって、金融取引中に電子マネーを一時的に維持するために用いられるもの、

(6) 外国為替勘定：各銀行により所有されるゼロバランス(残高なし)負債勘定であって、複数通貨の交換を処理するために用いられるもの、である。

【0185】コルレス銀行2において、

(1) 発行銀行預金勘定：発行銀行1におけるコルレス銀行2の口座の残高を反映する負債勘定、

(2) 金銭借入勘定：銀行口座に預金された金銭を反映する資産勘定、

(3) 外国為替勘定：各銀行によって所有される残高なし負債勘定であって、複数通貨の交換を処理するために用いられるもの、

(4) 通過金銭勘定：各銀行によって所有される残高なし負債勘定であって、金融取引中に電子マネーを一時的に維持するために用いられるもの、である。

【0186】決済銀行3において、

(1) 発行銀行1の清算勘定：発行銀行1のために清算された金額を総計する負債勘定、である。

【0187】それらの対応する略号を有する勘定は次のように要約される。

※に、典型的な取引及びそれらに関連する会計段階の幾つかの例を次に説明する。

【0189】すなわち、図11~24は預金、引出、外国為替、清算金の受領、電子マネー/現金交換、及び手形11の更新についての会計処理を示すものである。図11~14及び図19~22は、金銭取引モジュール4が特定の取引には含まれない手形11を収容しているときの会計手続の流れを示している。取引の部分をなすな

い手形11は分離され、前述した安全保障手続において、述べたような更新手形と置換される。例えば、加入者が彼の金銭取引モジュール4にストアされたものより少額の電子マネーを預金し、かつ清算しないで置く場合、その清算を表す電子手形11が最新の証明を含む電子手形11とされる。この後者の場合は、図11～14及び図19～22の挿入エントリにおいて示されている。

【0190】本発明による会計構造の一例において（図11参照）、加入者が彼の金銭取引モジュール4に収容された電子マネー100ドルから50ドルをコルレス銀行の金銭出納モジュール（ステップ1）に預金したとすれば、全100ドルの電子マネーが引出され、その内50ドルが最初に彼の顧客口座（“A”で指示する）に貸方記入されるとともに、残りの50ドルはコルレス銀行の通過金銭勘定に貸方記入され、さらに、コルレス銀行2の金銭借入勘定に計100ドルが借方記入される（図11における“IT”及び“MD”参照）。

【0191】電子手形11の100ドルが分離された後、手形11はコルレス銀行の金銭出納モジュール5から発行銀行1の金銭出納モジュール5に預金される（ステップ2）。この移転の達成において、コルレス銀行2における金銭借入勘定は100ドルを貸方記入されるが、発行銀行口座におけるその預金は100ドルを借方記入される。すなわち、発行銀行1はそのコルレス銀行金銭勘定に100ドルだけ貸方記入するとともに、その金銭借入勘定に100ドルを借方記入する。

【0192】ステップ3においては、更新された手形11が要求される。したがって、コルレス銀行2は発行銀行1からその金銭発行モジュール6より発せられた最新の証明を含む電子マネー50ドルの引出を要求する。この要求を支持するため、発行銀行口座の預金に50ドルが貸方記入されるとともに、その通過勘定から50ドルが借方記入される。発行銀行1はここでそのコルレス銀行の金銭勘定から50ドルを借方記入するとともに、その金銭発行勘定に50ドルを貸方記入する。

【0193】取引が完了すると、この50ドルは金銭発生モジュール6から発行銀行1の金銭出納モジュール5を通じてコルレス銀行2の金銭出納モジュール5に移転され、最後に金銭取引モジュール4に移される（ステップ4～6）。これらの全取引の総合結果は加入者の口座に預金された残り50ドルと新たに発行された電子手形11の50ドルが加入者の金銭取引モジュール4にここでストアされるということである。

【0194】選択的に、加入者が彼の金銭取引モジュール4において50ドルから開始してその全てを預金すると、得意先勘定は50ドルだけ貸方記入されると共に借入勘定は50ドルだけ借方記入される（図11のステップ1、挿入エントリー）。

【0195】移転される電子手形11が50ドルのみで

あれば、コルレス銀行2は借入勘定に50ドルだけ貸方記入し、発行銀行口座における預金は50ドルの貸方記入となる（ステップ2、挿入エントリー）。この金銭は後に決済されるため発行銀行1に預金され、ここでコルレス銀行金銭勘定は50ドルの貸方記入となり借入勘定は50ドルの借方記入となる。この状況においては更新された電子手形11の変換は必要でないため、預金及びそのコルレス勘定はステップ2において完了する。

【0196】コルレス銀行に代わって発行銀行1で電子マネー預金の会計を進めるときのプロセスは図12に示されている。先の典型的な取引におけると同額のドル勘定を用い、金銭取引モジュール4にストアされた電子マネーにおける100ドルのうちの50ドルが発行銀行の金銭出納モジュールに直接預金される場合（ステップ1）、得意先勘定（A）には50ドルが貸方記入される。同時に通過勘定における金銭に対して50ドルが貸方記入され、発行銀行1における借入勘定に100ドルが借方記入される。

【0197】金銭取引モジュール4にストアされた全100ドルが発行銀行の金銭出納モジュール5に移転されたので、金銭取引モジュール4には50ドルの更新手形を返還する必要がある。したがってステップ2に示す通り金銭出納モジュール5はその金銭発生モジュール6から50ドルを要求し、その通過金銭勘定に50ドルの借方記入を行うと共にその金銭発行勘定に50ドルの借方記入を行う。

【0198】これに応じて金銭発生モジュール6により50ドルが発生され、それは金銭出納モジュール5に移転され、そのモジュール5はこの電子マネーを金銭取引モジュール4に移転する（ステップ3～4）。

【0199】金銭取引モジュール4に50ドルのみがストアされていてその全額を預金するとき、得意先勘定Aは50ドルだけ貸方記入され、借入勘定は50ドルだけ貸方記入されてこの処理が終わる。これは図12のステップ1における挿入エントリーに示す通りである。

【0200】コルレス銀行からの引き出しの場合（図13参照）、コルレス銀行2において金銭取引モジュール4を用いる加入者により100ドルの引き出しが要求されると、加入者の口座すなわち得意先勘定（A）は100ドルだけ借方記入され、コルレス銀行2の通過金銭勘定は100ドルだけ貸方記入される（ステップ1）。この100ドルの引き出し要求はコルレス銀行2から発行銀行1に送られ、コルレス銀行の発行銀行預金勘定が100ドルだけ貸方記入され、他方その通貨金銭勘定が100ドルだけ借方記入される（ステップ3）。

【0201】次に100ドルの要求は発行銀行1の金銭出納モジュール5によって金銭発生モジュール6に送られる。したがって、コルレス銀行の金銭勘定は100ドルの借方記入となり、金銭発行勘定は100ドルの借方記入となる（ステップ4）。

10

20

30

40

50

【0202】ここで金銭発生モジュール6は100ドルの電子手形11を発生し、それを発行銀行1の金銭出納モジュール5及びコルレス銀行2の金銭出納モジュール5を介して金銭取引モジュール4に移転する(ステップ5~6)。

【0203】たとえば加入者が50ドルの電子手形11を収容した金銭取引モジュール4によって100ドルの引き出し要求を行ったとき、手形11は解除され、ここで金銭借入勘定が50ドルの借方記入となり、加入者の口座はさらに100ドルの借方記入となり、通過金銭勘定は150ドルの貸方記入となる(ステップ1の挿入エントリー)。

【0204】次に発行銀行1に50ドルが預金され、これによって金銭借入勘定が50ドルの貸方記入となり、発行銀行預金勘定が50ドルの借方記入となる。発行銀行1において、コルレス銀行金銭勘定は50ドルの貸方記入となるが、借入勘定は50ドルの借方記入となる(ステップ2、挿入エントリー)。

【0205】50ドルの手形11が取り除かれたので、ステップ3における引き出し要求は150ドルでなければならない。この要求は発行銀行預金勘定に150ドルの貸方記入を生じると共に、通過金銭勘定に150ドルの借方記入を行うものである(ステップ3、挿入エントリー)。

【0206】発行銀行においては金銭発生モジュール6から150ドルが要求され、コルレス銀行金銭勘定は150ドルの借方記入となり、金銭発行勘定は150ドルの貸方記入となる(ステップ4、挿入エントリー)。上記の通り、金銭発生モジュール6により発生した金銭(150ドル)は発行銀行1及びコルレス銀行2の金銭出納モジュール5を介して金銭取引モジュール4に移転される(ステップ5~6、挿入エントリー)。

【0207】発行銀行1からの引き出しは比較的少ない会計手続を伴うものである。ここで図14を参照すると、金銭取引モジュール4による発行銀行1からの引き出し要求は発行銀行1の金銭出納モジュール5によって加入者の口座(A)に100ドルの借方記入を行わせると共に、その金銭発生勘定に100ドルの貸方記入を行わせる(ステップ1~2)。

【0208】更新された100ドルの要求はここで発行銀行1の金銭出納モジュール5により金銭発生モジュール6に対してなされる。金銭発生モジュール6はその発生時において100ドルを発行銀行の金銭出納モジュール5に返還する(ステップ3)。この取引の完了時において、発行銀行1の金銭出納モジュール5は最新の証明を含むこの新たな100ドルを金銭取引モジュール4に単純に移転する(ステップ4)。

【0209】選択的に、金銭取引モジュールが100ドルの引き出し時において50ドルを収容しているとき(挿入エントリー)、この50ドルは取り除かれ、発行

銀行の通過金銭勘定は50ドルの貸方記入となり、借入勘定は50ドルの借方記入となる(ステップ1)。

【0210】ここで発行銀行1は金銭発生モジュール6から150ドル要求しなければならない。当然ながら得意先勘定は100ドルの借方記入となる。金銭発行勘定は新たな手形11が発生したとき150ドルだけ貸方記入され、通過金銭勘定は50ドルだけ借方記入される(ステップ2)。ここから、150ドルは発行銀行1の金銭出納モジュール5を介して金銭取引モジュール4に返還される(ステップ3~4)。

【0211】図15は発行銀行1との外国為替取引の場合を示している。この例においては、加入者は彼の金銭取引モジュール4にストアされた100ドルの電子マネーを60ポンドの英国通貨に交換することを望んでいる。発行銀行1の金銭出納モジュール5における預金は発行銀行1の外国為替勘定を60ポンドだけ貸方記入するが、その借入勘定は100ドルだけ借方記入される(ステップ1)。ここに、この100ドルは金銭取引モジュール4から金銭出納モジュール5に移され、このモジュール5は60ポンドを表す電子手形11が金銭発生モジュール6によって生成されることを要求する(ステップ2)。

【0212】発行銀行1において、外国為替勘定はここで60ポンドだけ借方記入され、金銭発行勘定は60ポンドだけ貸方記入される。金銭発生モジュール6により生じた60ポンドの電子手形11は金銭出納モジュール5に移され、このモジュール5はここで100ドルと60ポンドの両方をストアする(ステップ3)。次に金銭出納モジュール5から金銭取引モジュール4に60ポンドが移され、その結果金銭取引モジュール4には60ポンドの正味残高があり、金銭出納モジュール5には100ドルが残ることになり移転が完了する(ステップ4)。

【0213】コルレス銀行2において100ドルを60ポンドに為替取引するための会計手続は図16に示されている。金銭取引モジュール4は、この例においてはその100ドルをコルレス銀行の金銭出納モジュール5から60ポンドを購入するために用いることを要求される。コルレス銀行の外国為替勘定はこれによって60ポンドだけ貸方記入されるが、その借入勘定は100ドルだけ貸方記入される(ステップ1)。金銭取引モジュール4にストアされた100ドルはコルレス銀行2の金銭出納モジュール5に移され、これは発行銀行1の金銭出納モジュール5に対して60ポンドの引き出し要求を送信し、更にその外国為替勘定に60ポンドの借方記入を行うと共に、その発行銀行勘定における預金口座に60ポンドの貸方記入を行うものである(ステップ2)。

【0214】発行銀行1におけるコルレス勘定取引はコルレス銀行金銭勘定に60ポンドの借方記入を行うと共に、金銭発行勘定に60ポンドの貸方記入を行う(ステ

ップ3)。次に発行銀行の金銭出納モジュール5は金銭発生モジュール6が60ポンドを発生してそれを発行銀行の前記モジュール5に送ることを要求し、さらにそれはコルレス銀行2の金銭出納モジュール5に移転される(ステップ4~5)。60ポンドの手形11はここから金銭取引モジュール4に移されて、60ポンドの残高となり、他方コルレス銀行2の金銭出納モジュール5は100ドルの残高によって終了する(ステップ6)。

【0215】信用手形11の引き出し又は預金のための会計処理は図17に示すような幾つかの会計オペレーションを含んでいる。加入者が彼の貸付限度額から金銭を引き出すことを望むとき(ステップ1)、金銭発生モジュール6から金銭取引モジュール4に妥当な信用手形11が単純に転送され、顧客貸付限度は移転された金額分だけ減少する(ステップ2~4)。

【0216】選択的に信用手形11は加入者の金銭取引モジュール4により預金されるとき、加入者の口座は預金された金額だけ増加し、借入勘定は同額だけ借方記入される(ステップ1)。

【0217】発行銀行1による電子マネー決済の受領を含む会計オペレーションについて次に説明する。図18を参照すると、この例においては100ドルの電子マネーと100ドルの信用手形11が幾つかの発行銀行1間における残高を清算するため決済銀行3により決済されたものである。100ドルの電子マネー及び100ドルの信用手形は妥当な発行銀行1に移転される(ステップ1)。これに伴って、発行された50ドルの電子手形11は更に発行銀行1に預金される。この結果発行銀行1は加入者の口座Aに100ドルだけ借方記入し、発行銀行の金銭発行勘定を150ドルだけ借方記入し、借入勘定を50ドルだけ貸方記入し、更に発行銀行の決済銀行預金口座を取引完了のために200ドルだけ貸方記入する。

【0218】次に図19を参照すると、現金を発行銀行1において電子手形11と交換する会計例が示されている。この例においては、加入者は現金50ドルを50ドルの電子手形11に代え、それを彼の金銭取引モジュール4にすでにストアされた100ドルの電子手形11に加えることを望んでいる。

【0219】最初の取引において、現金50ドルは発行銀行1に預金され、発行銀行1は通過金銭勘定に50ドルの貸方記入を行い、現金勘定は50ドルの借方記入となる(ステップ1)。

【0220】次に、金銭取引モジュール4中の100ドルの電子手形11が取り除かれ、通過金銭勘定が100ドルの貸方記入となり、更に借入勘定が100ドルの借方記入となる(ステップ2)。

【0221】金銭出納モジュール5はここで金銭発生モジュールから150ドルの電子手形11を要求し、加入者に対し150ドルの電子手形11を返還する(ステッ

プ3)。したがって、金銭通貨勘定は150ドルの借方記入となるが金銭発生勘定は150ドルの貸方記入となる。

【0222】新たに発生した150ドルの電子手形11はここで金銭発生モジュール6から金銭取引モジュール5に移され、その150ドルは更に加入者の金銭取引モジュール4に移転される(ステップ4~5)。取引が完了すると加入者は150ドルの電子手形11を有し、発行銀行の現金勘定は50ドルの残高を含むことになる。

【0223】図19には更に加入者が50ドルの現金を電子手形11に変換し、彼の金銭取引モジュール4における残高がゼロとなる場合が示されている。ステップ1において、50ドルの現金は発行銀行1に預金され、銀行では通過金銭勘定が50ドルの貸方記入となるが、現金勘定は50ドルの借方記入となる。手形11が取り除かれた場合、ステップ2においては何らの会計も実行されない。

【0224】ステップ3においては、金銭発生モジュール6から50ドルだけ要求され、その結果、通過金銭勘定は50ドルの借方記入となるが、金銭発行勘定は50ドルの貸方記入となる。金銭モジュール間の同様の移転は50ドルのみが要求された前述の図19におけるステップ4~5と同様に発生する。これは加入者に彼の最初の所持貨幣50ドルの代わりに50ドルの電子手形11を付与するものである。

【0225】図20には、コルレス銀行2において現金を電子手形11と交換する態様が示されている。この例もまた図19におけると同様のパラメータが用いられる。すなわち加入者は50ドルの現金と彼の金銭取引モジュール4において100ドルの電子手形11を有するものとする。

【0226】現金50ドルがコルレス銀行2に預金されると、その通過金銭勘定は50ドルの貸方記入となるが、その現金勘定は50ドルの借方記入となる(ステップ1)。次に100ドルの電子手形11は金銭取引モジュール4からコルレス銀行2に移転され、そこでは通過金銭勘定において100ドルの貸方記入が行われると共に借入勘定に100ドルの借方記入が行われる(ステップ2)。

【0227】100ドルの電子手形11はそこから発行銀行1に預金され、その借入勘定が100ドルの借方記入となり、他方そのコルレス銀行金銭勘定が100ドルの貸方記入となる(ステップ3)。コルレス銀行2において、発行銀行預金勘定は100ドルの借方記入となるが、借入勘定は100ドルの貸方記入となる。

【0228】ここでコルレス銀行2により発行銀行1から150ドルを引き出す要求がなされる(ステップ4)。この要求はコルレス銀行2においてその通過金銭勘定を150ドルの借方記入とし、かつ発行銀行預金勘定に150ドルの貸方記入を行う。

【0229】これに対応して発行銀行1の金銭取引モジュール5は金銭発生モジュール6から150ドルの手形11を発行するように要求し、そのコルレス銀行金銭勘定を150ドルだけ借方記入すると共に、その金銭発行勘定を150ドルの貸方記入とする(ステップ5)。

【0230】最後に、150ドルの電子手形11は金銭発生モジュール6から発行銀行1の金銭出納モジュール5に移され、それは更にコルレス銀行2の金銭出納モジュール5を通過した後、金銭取引モジュール4に移される(ステップ6~8)。

【0231】選択的に、現金50ドルを有するが彼の金銭取引モジュール4には手形11を有しない加入者の場合が図20に示されている。最初の場合と同様、現金50ドルは発行銀行2に預金され、その通過金銭勘定は50ドルの貸方記入となるが、その現金勘定は50ドルの借方記入となる(ステップ1)。

【0232】ここで50ドルの引き出し要求が発行銀行1に対してなされ、通過金銭勘定は50ドルだけ借方記入され、発行銀行預金勘定は50ドルの貸方記入となる(ステップ4、挿入エントリー)。その後で金銭発生モジュール6から50ドルが要求されコルレス銀行金銭勘定は50ドルの借方記入となり、金銭発行勘定はステップ5において50ドルの貸方記入となる(挿入エントリー)。ここに、50ドルの電子手形11は上述したステップ6~8と同様の金銭モジュール通路を経て移転され、金銭取引モジュール4に到達する。

【0233】図21は電子手形11を発行銀行1において現金と交換する態様を示している。ここに加入者は彼の金銭取引モジュール4にストアされた100ドルの電子手形11を有し、その内の50ドルを現金50ドルと交換することを望んでいる。

【0234】金銭取引モジュール4が発行銀行1の金銭出納モジュール5との通信を確立した後、電子手形11の全100ドルは金銭取引モジュール4から取り除かれる(ステップ1)。これは通過金銭勘定に100ドルの貸方記入を行い、借入勘定(発行銀行1におけるもの)に100ドルの借方記入を行う。

【0235】金銭出納モジュール5はここで金銭発生モジュール6から更新された50ドルの電子手形11を要求し、この取引は通過金銭勘定において50ドルの借方記入を行うと共に金銭発行勘定において50ドルの貸方記入を行う(ステップ2)。新たに発生した50ドルの電子手形11はここで金銭出納モジュール5を介して金銭取引モジュール4に移転される。50ドルの現金は次に金銭出納手段すなわちATMを介して加入者に移転される(ステップ3~5)。

【0236】この図においては更に彼の金銭取引モジュール4に50ドルのみがストアされている場合の加入者がそれを同額の現金と交換する場合が示されている。発行銀行において、50ドルの電子手形11が取り除かれ

るために通過金銭勘定に50ドルの貸方記入がなされ、金銭借入勘定に50ドルの借方記入がなされる。次に50ドルの電子手形11しか預金していない加入者に対して50ドルの貨幣が返還される(ステップ5)。

【0237】この取引が完了するといずれの場合においても通過金銭勘定は50ドルだけ借方記入され、発行銀行1における現金勘定は50ドルだけ貸方記入される。その最終結果として、彼の金銭取引モジュール4において50ドルの更新された電子手形11が存在する前者の場合においてのみ、加入者が50ドルの現金を得ることができる。

【0238】電子手形11をコルレス銀行2において貨幣と交換する態様は図22に示されている。図21に示された実施例と同様、加入者は50ドルの電子手形11の交換のみを行うものであるが、電子手形11の全100ドルは加入者の金銭取引モジュール4から移転される(ステップ1)。

【0239】手形11が移転された後、コルレス銀行2の金銭出納モジュール5はその金銭通過勘定に100ドルの貸方記入を行い、その金銭借入勘定に100ドルの借方記入を行う。電子手形11のこの100ドルはここで発行銀行1に預金され、これによってコルレス銀行2はその金銭借入勘定に100ドルの貸方記入を行うと共に発行銀行預金勘定に100ドルの借方記入を行う(ステップ2)。

【0240】発行銀行21においてコルレス銀行金銭勘定には100ドルの貸方記入が行われるが、金銭借入勘定には100ドルの借方記入が行われる。ここでコルレス銀行2は発行銀行1から50ドルの電子手形11を引き出すことを要求する(ステップ3)。その結果、発行銀行預金勘定は50ドルだけ貸方記入されるが、コルレス銀行2における通過金銭勘定は50ドルだけ借方記入される。

【0241】ここで、発行銀行1の金銭出納モジュール5は金銭発生モジュール6から50ドルを要求すると共にそのコルレス銀行金銭勘定に50ドルの借方記入を行い、かつその金銭発行勘定に50ドルの貸方記入を行う(ステップ4)。更新された電子手形11の50ドルは金銭発生モジュール6から発行銀行1の金銭出納モジュール5及びコルレス銀行2の金銭出納モジュール5を介してステップ5~7において金銭取引モジュール4に返還される。

【0242】金銭取引モジュール4に50ドルしかストアされていない場合の同様の実施例もまた図示されている。これはコルレス銀行2において預金されたものであり貨幣に交換される場合である。この預金の場合、通過金銭勘定は50ドルの貸方記入を行われ、金銭借入勘定は50ドルの借方記入を行われる(ステップ1)。次に50ドルはコルレス銀行2によって発行銀行1におけるその口座に預金される。コルレス銀行2において、金銭

51

借入勘定には50ドルの貸方記入が行われ、発行銀行預金勘定には50ドルの借方記入が行われる。発行銀行1側において、コルレス銀行金銭勘定には50ドルの貸方記入が行われるが、金銭借入勘定には50ドルの借方記入が行われる。これは50ドルの預金が受け入れられた後である(ステップ2)。

【0243】2つの説明において、50ドルの現金はここでコルレス銀行2から加入者に移転され、同時にコルレス銀行2はその通過金銭勘定に50ドルの借方記入を行うと共に現金勘定に50ドルの貸方記入を行う(ステップ8)。加入者の手元には50ドルの現金が残る。これは最初の彼の金銭取引モジュール4に50ドルの電子手形11がストアされていた場合である。

【0244】図23は異なった発行銀行より発行された電子マネーを清算するための会計手順を示している。この図解は銀行Bから発行された100ドルの電子手形11が発行銀行Aに預金されていると共に銀行Aによって発行された150ドルの電子手形11が発行銀行Bに預金されている例である。

【0245】ステップ1において、発行銀行Aは銀行Bより発行された100ドルを決済銀行3に移転する。これにより発行銀行Aの金銭借入勘定は100ドルの貸方記入が行われると共に、決済銀行預金勘定には同額の借方記入が行われる。ステップ2において、発行銀行Bは発行銀行Aの金銭150ドルを決済銀行3に移転する。その発行銀行Bの金銭借入勘定は150ドルだけ貸方記入されると共に、その決済銀行預金勘定は150ドルだけ借方記入される。

【0246】合計で50ドルが銀行Bに支払うべきものであり、したがって、銀行Aの交換勘定には50ドルの借方記入がなされ、銀行Bの交換勘定には50ドルの貸方記入がなされる(ステップ3)。

【0247】図24には電子手形11の更新に対応する会計処理が示されている。ここに、金銭取引モジュール4には100ドルの電子手形11がストアされ、かつ発行銀行1に移転され、この場合通過金銭勘定には100ドルの貸方記入を行い、金銭借入勘定には100ドルの借方記入が行われる(ステップ1)。

【0248】100ドルの電子手形11は金銭発生モジュール6から要求されて通過金銭勘定に100ドルの借方記入を生じ、金銭発行勘定に100ドルの貸方記入を生じる(ステップ2)。この達成に伴って、100ドルの電子手形11は金銭発生モジュール6から発行銀行1の金銭出納モジュール5に移転される。その金銭は更に加入者の金銭取引モジュール4に移転される(ステップ3~4)。

【0249】調整及び決済システム

図25を参照すると、取引調整システム22が示されている。ここでは金銭出納モジュール5、金銭発生モジュール6及び銀行体系20が各参加銀行において維持され

52

た取引調整システム22に対し、取引レコードを周期的に送ることが理解されるであろう。これらの取引は分析及び照合されて本発明のシステムにおいて何らかの誤処理が発生しているか否かが判断される。

【0250】取引調整システム22は好ましくは適当な大きさを有し、かつ適当にプログラムされた汎用コンピュータにおいて具体化されるものであり、それは金銭出納モジュール5における金融的影響を伴う全ての取引、例えば預金、引き出し及び支払い、妥当な会計処理の照合等を保証するものである。何らかの不整合があればそれは不完全取引又は多分不正行為であると表示される。

【0251】金銭発生モジュール6によって発行された金銭を反映する取引は、また金銭出納モジュール5の取引に対応すべきであり、かつ妥当な会計処理レコードを有するべきである。何らかの不整合データは不完全な処理又は安全性の破綻として指示される。不整合な会計処理は不完全な取引又は銀行体系20のレコードに対する不正な試みにより生じるものである。

【0252】好ましい実施例において、これらの不整合取引は問題の原因を判断する検査システム12に転送される。検査システムが取引レコードに対する不整合を見直し、かつ状況を修正する適当な行為を判断することができるようにするため、オンライン対話を実施することができる。これにより検査システムは勘定を調整し、金銭出納モジュール5及び金銭発生モジュール6の誤動作を無効にし、更に加入者に修正行為を通知することにより修正作業を行うことができる。

【0253】ここで図26を参照すると、預金取引を取り扱うための清算プロセスが示されている。加入者の預金は発行銀行1における彼らの口座にリアルタイムで預金されるため、コルレス銀行はこの処理に含まれない。発行銀行において、預金は決済システム13により一括処理されて決済銀行3に送信されるための預金電子マネー(コルレス銀行からの預金を含む)に全て統合される。

【0254】決済銀行3は大量の取引及びシステムが典型的に取り扱うであろう対応するデータ量を許容する何らかのコンピュータ処理施設において具体化される。これには大容量メインフレームコンピュータ、適当サイズミニコンピュータシステム、必要なデータ処理容量を有する多数のネットワーク接続されたワークステーション又はそれらの結合が採用される。当業者によってよく認識される通り、決済銀行3のハードウェアシステムの特定の設計は本発明の要部ではない。

【0255】発行銀行1は幾つかの手続の一つにおいて金銭を清算することができる。これらの手続の一つにおいて、電子マネーは発行銀行1から決済銀行3にオンラインで預金させることができる。これは取引が実際に行われているときにリアルタイムモードにおいてオンライン処理される。選択的に、発行銀行1は後にバッチ処理

(又はオフライン処理)する日までの間に実行される取引の詳細を記録することができる。銀行間処理は1日に数回行われる。

【0256】図26に示す通り、発行銀行1はその電子マネーを預金調整ファイル(調整預金)に周期的に転送する。このファイルは処理された後決済銀行3に伝達される。このファイルからの取引レコードは、統計及びハウスキーピング機能のために銀行の取引調整システム22に転送される。

【0257】決済銀行3においては、預金調整ファイルが処理され、各発行銀行1の営業性預金毎に通貨単位による借方記入又は貸方記入を生じる。当然ながら、これらの営業性預金に対する適当な会計処理は決済処理中において明示される。何らかの貸越勘定があればそれは一般に用いられている通常の銀行間決済処理によって清算されるであろう。

【0258】清算されるように処理された電子マネーはそれを発行した各銀行の金銭発行調整システム23に返送され、不正及び複製行為について調整及びチェックされる。

【0259】統計的機能及びハウスキーピング機能は図27に示された金銭発行調整システム23において具体化される。発行銀行1は典型的には汎用コンピュータにおいて具体化されたそれら自身の金銭発行調整システム23を装備し、発行された電子マネーを決済銀行3において決済された電子マネーと照合する。

【0260】図27に示された通り、発行銀行1において発行された電子マネー及び預金された電子マネーと、決済銀行3から受け取られた金銭清算取引は金銭発行調整システム23に転送される。金銭発行調整システム23は清算された金銭に対する会計取引を発生し、かつ発行された全ての銀行マネーのマスターファイルを更新する。更に銀行発行システム23は検査サブシステム13に清算されたが発行されなかったか、又は多分2回以上移転されなかった金銭を送信する。

【0261】何らかの不整合が生じた場合は安全性の具体的な破綻として明示される。検査システムは次に金銭発生モジュール6が妥当に動作していないか、又は金銭モジュールが不正に動作しているかということを判定することができる。誤用又は濫用された金銭モジュールのモジュール認識番号は各銀行の安全保障手段27に送られ、銀行のローカルネットワーク28における他の金銭モジュールに分配される。この認識番号は更にネットワーク25中に適当に分配されるため証明機関28に送られる。

【0262】金銭発行マスターファイルは個別的に金融状態システム24によりアクセスされる。このシステム24は統合された金融状態を発生するために決済銀行3に伝達されるべきファイルを生成する。全ての発行銀行1は特定の期間の終了時、典型的には一日の終わりにそ

れらの位置を判定するレポートを提供する。金融状態システム24はこれらのレポートを統合して発行銀行1により発行された各通貨単位毎の金額を掌握する。これらのレポートは銀行間決算問題のリスクを評価するために各発行銀行1の顕著な位置を反映するものである。

【0263】オペレーションシーケンス

好ましい実施例の幾つかの局面は詳細な線図を用いて説明されるが、その取引機能はプロセスフローチャートを用いて最もよく説明される。すなわち、金銭モジュールのオペレーションに対する理解を容易にするため、図28~図68のフローチャートにおいて幾つかの取引例が図解されている。これらの図を参照して以下本発明の好ましい実施例の原理を取り入れたシステム処理及び関連するアプリケーション機能を詳細な説明を進めることとする。

【0264】フローチャートの記述(例外を含む)を通じて、携帯用装置又は他の形式の処理装置に組み込まれた金銭取引モジュール4のアプリケーション機能はこれ以後添字“A”で指示し、金銭出納モジュール5のアプリケーション及びその関連銀行については以下添字“B”で指定することとする。コルレス銀行2が発行銀行1と相互作用するとき、発行銀行1またはコルレス銀行とその関連する金銭出納モジュール5のアプリケーションは以下“C”で指示することとする。

【0265】更に、ある図から別の図へのステップの移動は英数字記号を有する五角形タグによって指示し、また他の図への続きは同一の英数字記号を有する円で指示することとする。

【0266】発行銀行からの引き出し

図28~45には、金銭取引モジュール4と金銭出納モジュール5との間の取引のプロセスフローチャートが示されている。このプロセス例において、加入者は参加銀行との通貨取引を完了すること、特に彼の口座から幾らかの金額の電子マネーを引き出して彼の金銭取引モジュール4にストアすることを望んでいるものとする。

【0267】引き出し処理をセットするプロセスフローは図28の頂上部において開始する。第1のフロップロックは金銭モジュールAと銀行の金銭出納モジュールB5との間でセットされる引き出しであり、これは図29において更に説明される。このプロセスは金銭モジュールAがサイン記入処理を行うことから開始する。これについては別の図、特に図32において詳細に説明する。

【0268】加入者のサインオン(機械的サイン記入) 図32の頂部を参照すると、加入者が彼の金銭取引モジュール4を用いてサインオン機能(ステップ10)を実行する態様が示されている。期間管理アプリケーション32はサインオンメッセージを受信し(ステップ12)、更に金銭取引モジュール4がサインオンを禁止された加入者を有するか否かをチェックする(ステップ14)。

55

【0269】加入者のサインオンは両者が金銭取引モジュール4に何回かの不首尾なサインオンを試みた場合に禁止されうる。例えば、許容されるサインオンの試みは3回に限られ、もし何者かが金銭取引モジュール4に対して連続して4回以上金銭取引モジュール4にサインオンを試みた場合、期間管理手段31はそれ以上のサインオンの試みを禁止する。更に、このような“ロックアウト”機能は、例えば24時間程度の所定時間内だけ維持される。このような構成は金銭取引モジュール4を所持したが、その使用について妥当な権限を有しないものによってそのモジュールが使用されることから保護するものである。

【0270】この形式の構成は本発明の好ましい実施例において想定されるものであるが、本発明はそれに限定されるものではない。すなわち無権限者の侵害から安全保障する技術としてこの分野において周知された幾つかの方法をここに用いることができるからである。

【0271】典型的な場合としてサインオンがまだ禁止されていないならば、対加入者アプリケーション34は加入者をして彼のサインオン特性、すなわちPIN及びその個体的特徴を打ち込ませる(ステップ22)。加入者からの入力は期間管理手段31を通じて対加入者アプリケーション34に送られる(ステップ24~28)。これは入力された特性に回答して金銭取引モジュール4のメモリー中に記憶されたものと比較して加入者の認識特性が正確であれば、その加入者が金銭取引モジュール4を取り扱う状態にする(ステップ30~32)。

【0272】もし加入者の認識特性がメモリーにストアされた認識特性と整合しなれば、対加入者アプリケーション34は無効なサインオンを行った加入者に警告する(ステップ34)。対加入者アプリケーション34はここから利用者がサインオンを何回試みたかをチェックし(ステップ36)、それが所定カウントに到達しなければ期間管理手段31が警告される(ステップ38)。

【0273】期間管理手段32はクロック/タイマー43と関連動作して何回かの不首尾なサインオンの試みにおいて経過した時間をセット及び監視する(ステップ40)。一実施例においては設定時間周期内に異常に多い不首尾サインオンの試みがあった場合には、期間管理手段32がそれ以上のサインオンを禁止して金銭取引モジュール4を有効に使用できないようにする。期間管理手段32はサインオンが終了したことをステップ42において認識する。

【0274】再び図32のステップ14に戻ると、金銭取引モジュール4が禁止されたものとして、期間管理手段32は所定の時間周期が終了したか否かをチェックする(ステップ16)。もし金銭取引モジュール4がなおサインオン禁止モードにあれば、対加入者アプリケーション34は加入者に対し金銭取引モジュール4へのこれ以上のアクセスが禁止されるというメッセージを送る

56

(ステップ18~20)。期間管理手段32はここでサインオンの試みが終了したことを認識しステップ32に戻る。

【0275】引き出しの設定

図29に返ると、正確なサインオンが行われなかった場合、対加入者アプリケーション34は加入者が所望の取引を実行できるようにする(ステップ43)。前述した通り、加入者は幾つかの異なった参加銀行及び金融機関における複数の口座のいずれか一つと取引することができる。

【0276】特定の銀行及び口座が選択された後(ステップ44)金銭取引モジュール4はネットワーク25を接続することにより選択された銀行との通信手続を開始する。ここで全体のプログラムフローが図35におけるフローチャートとして示された手続を辿る。図35にはネットワーク25に対するサインオンを具体化するデータ処理及び流れが示されている。

【0277】ネットワークサインオン

以下に説明する図示のネットワーク25のサインオン方法は一般に本発明の実施例の金銭モジュール4、5、6のいずれかに適用することができる。そこでこの例において、“A”はいずれかのクラスの金銭モジュールを表すものとする。

【0278】アクセスされるべき銀行が選択された後、金銭モジュールはその期間管理手段A31の制御を受けてネットワーク25との通信を開始する(ステップ50)。ネットワークサービス手段26は期間管理手段A31から金銭取引モジュール4の証明を要求することにより動作を開始する(ステップ52~54)。安全維持アプリケーションA37は期間管理手段A31に対して証明を検索し、かつ送信する(ステップ56)。期間管理手段A32はネットワークサービス手段26に証明を送り(ステップ58)、ネットワークサービス手段は受信に基づいてその証明を安全保障手段27に供給する(ステップ60)。

【0279】安全保障手段27は証明を検索してその有効性をチェックし(ステップ62~64)、それが何らかの理由で無効であれば、ネットワークサービス手段26にアクセスを否定する信号を送る(ステップ66)。ネットワークサービス手段26は更にアクセス否定メッセージを金銭取引モジュール4の期間管理手段Aに転送する(ステップ68~70)。

【0280】アクセス否定メッセージを受け取った期間管理手段Aが金銭取引モジュール4のものであれば、その対加入者アプリケーションAは加入者にこの条件を告知する(ステップ74)。金銭取引モジュール5又は金銭発生モジュール6がネットワーク25にアクセスすることを試みている場合、対銀行アプリケーションA47は銀行体系20にそのアクセスが許されないことを告知する(ステップ76)。

【0281】証明の有効性チェックが満足なものであれば、安全維持サービス手段27は好ましくない金銭モジュールの更新リスト及び証明キーの新たなリストを期間管理手段Aに送信する(図36、ステップ78)。これらのキーは証明キーの最終編を用いてサイン記入操作される。この情報は期間管理手段Aに受信されると共に安全維持アプリケーションA37に送られ、このアプリケーションは証明キーリスト及び好ましくない金銭モジュールリストを有効化する(図36、ステップ80～82)。

【0282】パブリックキーA44は署名の有効性をテストし(ステップ84)、その署名が有効でなければ金銭取引モジュール4の対加入者アプリケーションA33により(ステップ86～90)、又は選択的に金銭出納モジュール5または金銭発生モジュール6の対銀行アプリケーションA47により(ステップ86～88、92)、ネットワーク安全問題に関する警告メッセージが発せられる。便宜上、全ての金銭モジュールは等しく安全保障手段27から受信された署名の有効性をチェックする。これはシステム全体の完全性を保証するための補助となる。

【0283】署名が有効であれば、安全維持アプリケーションAは好ましくない金銭モジュールのリスト及び証明キーリストを更新する(ステップ94)。証明自体が再保証されるべきであるか又は証明期間が終了したならば(ステップ96及び98)、安全維持アプリケーションAは新たな証明を発生し(図38のステップ126)、パブリックキーAは新たなキーを発生し、かつ古いパブリックキーを用いて証明サインを行う(ステップ128)。期間管理手段Aは新たな証明を安全保障手段27に送信し、この手段27は証明を受け入れて署名の有効性をテストする(ステップ130～136)。

【0284】新たな証明の署名がこの段階において有効でなければ、図35のステップ66～76が繰り返されてネットワーク25への通信リンクを終了させるようにする。

【0285】他方、図38において有効な署名が安全保障手段をして新たな証明をサインせしめると共に、それを金銭モジュールに返送せしめる(ステップ138)。期間管理手段A31は図39のステップ140において新たな証明を受け取り、それをその安全維持アプリケーションAに送り、パブリックキーアプリケーションを用いてその証明を再び有効化する(ステップ142～146)。ここに金銭モジュールは安全保障手段27から発行された証明の有効性テストを繰り返す。有効な署名の場合、期間管理手段A32は安全保障手段27に承認票を送り(ステップ148)、その手段27は図36のステップ78にプロセスを復帰させることにより応答する。

【0286】逆に、金銭取引モジュールAにより発生し

た新たな証明における安全保障手段の署名が無効であれば、図39において期間管理手段Aは安全保障手段27にその証明を返送することと相まって証明無効メッセージをも送信する(ステップ150)、この手段は再び証明上の署名を有効化するように試みる(ステップ152)。有効な署名はプロセスを図35のステップ66に復帰させる。選択的に、無効な署名は安全保障手段27をしてネットワーク25から切り離させ(図39、ステップ156)、ネットワークサービス手段26をして金銭モジュールに誤動作の警告を行わしめる(ステップ158)。

【0287】メッセージを受信した(ステップ160)期間管理手段Aが金銭取引モジュール4のものであれば、それは対加入者アプリケーション33に彼らがネットワーク25に対してサインオンを行う全プロセスを再び試みようとするか否かを質問させる(ステップ164及び168)。金銭出納モジュール5または金銭発生モジュール6のものである場合においては、対銀行アプリケーションAはネットワーク25がサインオン手続を再び試みようとするか否かを質問する(ステップ166及び168)。

【0288】もちろん、再試行が望まれない場合にはネットワーク25への通信リンクは終了し、逆にネットワーク25のアクセスに関する再試行要求があれば、それは手続を図35のステップ56に戻し、ここで、安全維持アプリケーションAは再びネットワークサービス手段26に関する金銭取引モジュールの証明を検索する。

【0289】証明が再保証されることを要求されないか又は消滅した場合、プロセスは図36のステップ98に戻り期間管理手段A32はクロック/タイマAから(図37、ステップ102)日時を要求し(ステップ100)、このデータをネットワークサービス手段26に送る(ステップ104)。

【0290】ネットワークサービス手段26が日時をその受信後においてチェックすると(ステップ106)、それがもし許された所定のパラメータから外れていれば、ネットワークサービス手段26は新たな日時(ステップ110)を期間管理手段Aを通じてクロック/タイマAに送る(ステップ112及び114)。もしクロック/タイマA43が日時をネットワーク25と同期化するように調整できなければ、加入者又は銀行のための金銭モジュールのオペレータはクロック誤動作の警告を受ける(ステップ116～124)。

【0291】オペレータは明確な誤動作にตอบสนองして、ステップ124においてネットワークサービス手段26から再び送られてくる日時を取得することができ、手続はそこでステップ102に戻って金銭モジュールに新たな日時を送ろうとする。逆に受入れ可能な日時をチェックされればシステムはステップ108においてネットワークサービス手段26及び期間管理手段Aが承認票を交換

し、かつ有効なネットワーク25のサインオンを認識する(ステップ126~128)。

【0292】期間Aの設定

図29に示す通り、金銭モジュールのサインオンステップが終了すると、取引選択及びネットワークサインオンが完了し、金銭モジュール間で期間が設定される。図40は金銭モジュール対金銭モジュール期間を設定するためのフローチャートであり、本発明の種々の形式の金銭モジュール間における他の期間設定に対しても良く適用可能であることが理解されよう。

【0293】図40の頂上部を参照して、期間管理手段Aはまず加入者がネットワーク25内の特定の行先に接続されることを要求しているか否かをチェックする(ステップ190)。例えば、加入者が特定銀行における彼の口座による取引を望む場合、ネットワーク25は金銭取引モジュール4を選択された銀行に接続する(ステップ192~198)。逆に、加入者がネットワーク25における更新機能を実行しているときは、いかなる特定銀行との取引期間設定をも必要とせず、したがってネットワークサービス手段26はネットワーク25のトラフィックに基づいて接続を導くところを決定することができる。

【0294】特定の行先が加入者によって選択された場合、期間管理手段Aはその行先情報をネットワークサービス手段26に転送する(ステップ194)。ネットワークサービス手段26は選択された行先の金銭モジュールに対する通信リンクを開始し(ステップ196)、期間管理手段A32に承認票を送る。

【0295】目指す行先の金銭モジュールが接続された(ステップ198)ことの承認票を受信した後、安全維持アプリケーションAはその証明を各アプリケーションの対応する期間管理手段を介して安全維持アプリケーションBに送信する(ステップ200~206)。

【0296】金銭モジュールは証明を交換して各金銭モジュールが別の有効な金銭モジュールと接触していることを検証する。この結果(図41参照)、パブリックキーアプリケーションB44はパブリックキーアルゴリズム及び金銭モジュールAに用いられたプライベートキーに対応するパブリックキーを使用することにより、金銭モジュールAの証明をテストし、Aの証明を暗号化しつつチェックすると共に、それが有効であることを検証する(ステップ208)。

【0297】証明が無効であることを発見されると、期間管理手段Bは期間が終了したことを認識する(ステップ210)。金銭取引モジュール4の場合において、対加入者アプリケーションBは加入者に取引終了を通知する(ステップ212)。同様に金銭出納モジュール5又は金銭発生モジュール6は対銀行アプリケーションB47に取引が終了した銀行を通知する(ステップ213)。ここで相手先金銭モジュールはタイムアウトして

交換を終了する。

【0298】図41のステップ214において金銭モジュールAの証明が有効であるものとし、安全維持アプリケーションB37は金銭モジュールAが妥結した金銭モジュールのリスト上にあるか否かをチェックする(ステップ215)。金銭モジュールAがそのリスト上にあれば、プロセスフローはステップ210に復帰し通信を終了することができる。

【0299】他方、金銭モジュールAが妥結した金銭モジュールのリスト上になければ、乱数発生アプリケーションB46が期間キーを発生する(ステップ216)と共にその期間キーを金銭モジュールBの証明及び検証メッセージと共にエンコードする。これには金銭モジュールAのパブリックキーが用いられる(ステップ218)。このコード化メッセージは期間管理手段B32により金銭モジュールAに送られる(ステップ220)。【0300】期間管理手段A31は金銭モジュールBからメッセージを受信し(ステップ222)、そのパブリックキー44のアルゴリズムアプリケーションを用いてメッセージをデコードし(図42、ステップ224)、かつ金銭モジュールBの証明を検証する(ステップ226)。

【0301】テストにより金銭モジュールBの証明が無効であると判定されれば、オペレーションは“取引中止”手続に分岐し、期間設定のために取られた全ステップを終了する(ステップ500~524)。この手続は、例えば通信期間を終了して金銭モジュールAの機能的遮断を行い、その結果通信リンクを終了するために用いられる(図34、ステップ500~524)。

【0302】取引中止

図34を参照して、取引中止プロセスを通じて行う金銭モジュールの機能的遮断につき説明する。いずれか2個の金銭モジュールが両者間で発生した取引を異常な形で終了したときには、次のプロセスが用いられることが理解されるであろう。したがって、金銭モジュールはプロセス段階の一般適用性を示すために“X”及び“Y”で指示することとする。

【0303】金銭モジュールYとの通信を終了するために金銭モジュールXにより開始された取引中止プロセスは、期間管理手段X31が金銭モジュールに対してなされた何らかのプログラム変化をとらえて、これを反転又は復元し(ステップ400)、さらに、期間が中止したことを認識する(ステップ502)ことを開始させる。

【0304】通信終了を開始しようとする金銭モジュールが、金銭取引モジュール4である場合において、対加入者アプリケーション33は、加入者に通信の終了を通知する(ステップ510)。同様に、金銭出納モジュール5は、その対銀行アプリケーション47に終了を通知し、これによって何らの会計変化も行われなくする(ステップ508)。次に、終了する金銭モジュールの期間

61

管理手段X31は、関連する他の金銭モジュールにコード化メッセージを送信する（ステップ512）。

【0305】図48を参照すると、モジュール間の全暗号化メッセージは、次のステップによって交換されることになる。送信側金銭モジュール（ここでもまた“X”として指示する）はその対称キー45を用いてメッセージを受信側金銭モジュール（ここでもまた“Y”として参照する）に送信すべくエンコードする（ステップ2）。これには周知の多数の暗号化技術を採用し得ることが認識されよう。

【0306】期間管理手段X32は、コード化メッセージを期間管理手段Y32に送信し、この手段32はその対称キーY45を用いてメッセージをデコードする（ステップ4〜8）。

【0307】図34を引続き参照して、期間管理手段Yは、期間を設定するために意図された何らの変更も行わないことにより期間中止を認識し、これによって終了通知に応答するものである（ステップ514〜516）。もし、遮断中のものが金銭取引モジュール4であれば、対加入者アプリケーション33は加入者にその状態を警告する（ステップ518及び524）。これに対応して金銭出納モジュール5においては、対銀行アプリケーション47が、試みられたすべての会計取引を覆すことになる（ステップ518〜522）。

【0308】図42を参照して、金銭モジュールBの証明が有効であるものとすれば、安全維持アプリケーションAは、ステップ228において金銭モジュールBが妥結した金銭モジュールのリスト中にあるか否かをチェックする。そして、金銭モジュールBがそのリスト中にある（ステップ230）、期間は取引中止手続に戻る（ステップ500〜524）。通信期間はその後解除される。

【0309】より典型的な場合、金銭モジュールBは妥結した金銭モジュールのリスト中に存在せず、クロック/タイマA43は日時を検索する（ステップ232）と共に、この情報を安全維持アプリケーションA37に送り、これによって日時と検証メッセージとが組み合わされる（ステップ234）。

【0310】対称キーA45はここで検証メッセージを日時情報と共に暗号化する。これには金銭モジュールBにより提供されるランダム期間キーが用いられる（ステップ236）。期間管理手段A32はこの暗号化メッセージ（ステップ238）を期間管理手段B32に送信する（ステップ240）。対称キーアプリケーションB45は、この状態から暗号化メッセージを解読し（ステップ242）、それをメッセージを検証するために安全維持アプリケーションB37に送る（図43、ステップ244）。不正確なメッセージはステップ500〜524を経て期間を中止させるものであるが、正確なメッセージは手続を進ませ、これによって安全維持アプリケーション

62

ョンB37はその日時を金銭モジュールAの日時と比較することができる（ステップ248）。

【0311】クロック/タイマB43は、金銭モジュールAのクロックが金銭モジュールBのクロックからの所定変位量内にあるか否かを検証する（ステップ250）。もし、両クロック間相互のずれが所定量より大きいという不一致があれば、期間はステップ500〜524に分岐することにより中止される。

【0312】もし、ずれが所定量より大きいという不一致がなければ、期間管理手段B32はその期間の開始を認識し（ステップ252）、その認識票を金銭モジュールAに送って取引を開始させる（ステップ254）。コード化されたメッセージがプロセスステップ2〜8（図48）を用いて金銭モジュールBから期間管理手段A31に送られた後、期間管理手段A31はそのメッセージ受領を承認して期間の開始を認識する（ステップ256〜258）。

【0313】引出し要求

金銭取引モジュール4と金銭出納モジュール5との間に期間が設定された後、金銭取引モジュール4は図29に示すように金銭出納モジュール5からの引出し要求を行う。ここで図30を参照して、引出しを要求するプロセスについて説明する。図は以下に説明したプロセス段階において、取引部門を“X”及び“Y”で指示するものであるが、それらは金銭出納モジュール5と取り引きするいかなる金銭モジュールに対しても適用できるものである。

【0314】まず、対出納アプリケーションX34は、金銭出納モジュール5に引出し要求を送り、特定口座から引出すべき金額を要求する。引出し要求の送信において、口座番号及び口座プロフィールが、要求を発する金銭モジュールから金銭出納モジュール5に伝達される（ステップ700）。この要求を送るため、プロセスステップ2〜8が繰り返される。この場合、メッセージは前述した暗号化技術を用いて暗号化される。

【0315】口座番号の有効化

一度、引出し要求と口座番号及び口座プロフィールが金銭出納モジュール5に伝達されると、口座番号を有効化する手続が開始される（ステップ7041〜7056）。口座番号を如何にして有効化するかを描いたフロー線図は図49に示されている。

【0316】このプロセスにおいて、金銭出納モジュール5の安全維持アプリケーション37は、口座番号及び署名を受信し、それらをそのパブリックキーアプリケーション44に転送してプロフィール署名を検証する（ステップ7041〜7042）。署名は銀行の安全保障手段27により発生し、かつ、分配されたパブリックキーを用いてテストされる。署名が有効なものでなければ安全維持アプリケーション37が期間管理手段にその口座プロフィールは無効であることを告知し（ステップ70

63

44)、これによって図34におけるステップ500～524が実行され、2つの金銭モジュール間の取引が中止される。

【0317】署名テストが有効な署名であることを確認した場合、手続は対銀行アプリケーション47に進み、このアプリケーションは受信された口座番号を銀行のコンピュータシステムに送信する(ステップ7046)。その口座番号が非活動口座であれば、安全維持アプリケーション37が期間管理手段に、それが非活動口座であることを告知し(ステップ7048)、ステップ500～524を辿って取引の中止がなされ、逆に非活動でない口座は安全維持アプリケーション37により口座プロフィールが再証明されるべきであるか否かをチェックする(ステップ7047～7050)。

【0318】口座プロフィールが再証明されるべきであれば、安全維持アプリケーション37は口座プロフィールを安全保障手段27に送り(図50、ステップ7051～7052)、この手段は口座プロフィールを再証明し、かつ、それを金銭出納モジュール5に送信する(ステップ7053)。金銭出納モジュール5はこれに回答してその口座プロフィールを金銭モジュールに送り、引出し要求を行う(ステップ7054)。

【0319】金銭出納モジュール5から金銭モジュールへの通信は、メッセージを送るために前述したルーチン(ステップ2～8)を利用する。ここで安全維持アプリケーション37は、その金銭モジュールにおける口座プロフィールを更新し、かつ、金銭出納モジュール5における安全維持アプリケーション37に承認票を返送する(ステップ7055)。これはまた、ステップ2～8を用いるものである。電子メッセージは金銭出納モジュール5の安全維持アプリケーション37により受信され、ステップ7056において承認される。

【0320】口座情報がチェックされると、プロセスは図30のステップ704に戻る。ここで対銀行アプリケーション47は、引出し要求を支持するに十分な資金があるか否かを検証する(ステップ704)。十分な資金があれば、金銭取引モジュール4に認識票を返送させ、プロセスステップ2～8を用いて認識票をその対出納アプリケーション34の機能(ステップ706～714)に対して送信する。金銭出納モジュール5の場合においては承認票が要求されない。

【0321】金銭取引モジュール4の場合において、資金量が不十分であれば、それは加入者が引出しのために新たな金額を入れるように送信する(図31、ステップ718～720)。ステップ724において示す通り、新たに入力された金額は、対出納アプリケーション34が金銭出納モジュール5の対銀行アプリケーション47(ステップ2～8を用いる)に対して新たな要求を送るようにし、これによって最新の要求額に見合った十分な資金が存在するか否かを検証し、図30のステップ70

64

4に復帰する。新たな要求額がなお銀行の残高における資金より大きい場合、金銭出納モジュール5はステップ500～524を開始して2個の金銭モジュール間の取引を中止させる。金銭出納モジュール5の場合においては、取引が貸越勘定となることを許容する。

【0322】手形の移転

図29に戻ると、対出納アプリケーションA34は、その通貨手形11のすべてを金銭出納モジュール5に移転する(ステップ45)。もし、引出し要求がなされた時点で金銭取引モジュール4に何らの手形11も保持されていないならば、対出納アプリケーションA34は金銭出納モジュール5に現在何らの手形11も存在しないというメッセージを送る(ステップ47)。これはプロセスステップ2～8を用いるものである。

【0323】電子手形11は後述の(及び図51に示す)手続を用いて金銭モジュール間で移転される。送り主の金銭モジュールにおける手形ディレクトリ(又は手形登録簿)アプリケーション39は、移転のための正確な値を有する手形を選択し(ステップ750)、かつ、手形アプリケーション40を有して各手形11の移転を承認する(ステップ752)。パブリックキーアプリケーション44は、すべての手形11のための署名を発生し(ステップ754)、これらの手形11をバケット管理アプリケーション41に送信し、手形11の移転及び署名をバケットとして組合せ、要求を発している金銭モジュールに送る(ステップ756)。

【0324】電子手形11のバケットを、受領及び分解(ステップ758)するために要求を発する金銭モジュールのバケット管理アプリケーション41に転送するため、ステップ2～8が用いられる。検証アプリケーション42は、証明に付随する移転を検証すると共に、総額が送られるべき手形11に一致することを検証する(ステップ760)。

【0325】何らかの無効情報があれば、前述したステップ500～524において概括される手続を用いて(ステップ761)、2個の金銭モジュール間の取引を中止する。有効な手形11はそれが手形11を転送した金銭取引モジュール4であるとき、検証アプリケーション42によってチェックされた(ステップ762)満了日を持つことになる。満了した手形11は(ステップ764)、図34のステップ500～524において概括された手続を用いて期間を中止させる。

【0326】手形11が満了しないか、又は金銭出納モジュール5がそれらを受け入れる場合、プロセスフローは図52のステップ765に復帰する。このステップにおいて、パブリックキーアプリケーションY44はデジタル署名を検証する。無効な署名はステップ500～524の取引中止プロセスを発動させる。

【0327】有効な電子手形11はここで手形アプリケーション40に送られ(ステップ768)、更に手形デ

65

ィレクトリアアプリケーション39が新たな手形位置及び量によって更新される(ステップ770)。

【0328】図28に戻ると、対取引アプリケーションB49は、いずれかの手形11が移転されたか否か(ステップ772)、及び手形11が金銭取引モジュール4から実際に移転されたか否かをチェックし、対銀行アプリケーションB47によりこの状況を反映するために会計取引が行われる(ステップ776及び図14のステップ1)。手形11が金銭モジュールから移転されなかった場合、及び後の会計取引がステップ776において確立された後において、金銭出納モジュール5と金銭発生モジュール6との間には、図40、図41～43のステップ190～258における前述した手続を用いて期間が設定される。

【0329】引出しを満足するために手形11が要求されるときは、この要求を反映する勘定が明示される。対銀行アプリケーションB47は、図14のステップ2に示したような妥当な会計取引(図28、ステップ778)を明示する(図28、ステップ778)。

【0330】手形の要求

図53を参照すると、手形11は以下に述べる手続を用いて金銭出納モジュール5及び金銭発生モジュール6間において要求される。

【0331】要求を発する金銭出納モジュール5の対金銭発生アプリケーション48は、発生されるべき電子手形の特定の金額について要求を発する(ステップ780)。この要求は暗号化送信について前述したステップ2～8を用いて金銭発生モジュール6の対出納アプリケーション34に送られ、これによって金銭発生アプリケーション50が活動状態となり(ステップ784)、電子手形11を発生する(ステップ786)。

【0332】電子手形11が発生した後、それらは金銭発生モジュール6のパブリックキーアプリケーション44によりサインされ(ステップ788)、かつ、その手形アプリケーション40によりホルダ中に置かれる(ステップ790)。最後に、手形ディレクトリアアプリケーション39は、新たに発生した電子手形11に関する情報により更新される(ステップ792)。

【0333】プロセスフローは、ここで図28に示す手続に復帰する。金銭発生モジュール6において要求された手形は、電子手形11を移転するために前述したプロセスステップ750～770を用いて金銭出納モジュールB5に移転される。次に手形11は、金銭出納モジュール5から金銭取引モジュール4に移転される。この移転には電子手形11を移転するための前記ステップ750～770が用いられる。

【0334】最後に、電子手形11の引出しを成功裏に終えるため、金銭モジュールは次の手続を用いることにより取引を委託し、もしくはそれを完成させる。ここで、図54を参照して、このプロセスの詳細を説明する

66

と、TLMアプリケーション36は、そのTLを更新して発生した取引を記録する(ステップ690)。交換を委託する(ステップ691)ものが金銭取引モジュール4であれば、対加入者アプリケーションが加入者に対し取引は成功裏に終了したということを告知する(ステップ692)。当然ながら、期間管理アプリケーションA32は、期間の終了を認識し(ステップ693)、かつ、プロセス2～8を採用して、それが取引関係にある金銭モジュールにメッセージを送る。この期間終了通知が受信されると、他の金銭モジュール、この実施例においては金銭出納モジュール5が、そのTLMアプリケーション36を用いてそれ自身のTLを更新する(ステップ694)。しかしながら、期間終了通知を受信する第2の金銭モジュールが、金銭出納モジュール5でないものとするれば、対加入者アプリケーション33を有する付加的なステップが、加入者に取引終了の生じたことを告知することが必要となる。いつの場合においても、第2の金銭モジュールの期間管理手段31は、期間終了の認識をも行うものである(ステップ698)。

【0335】図28に再び戻ると、委託すべきプロセスは、まず金銭取引モジュール4により開始されて金銭出納モジュールB5との取引を委託する(ステップ690～698)。プロセスステップは更に金銭出納モジュールB5と金銭発生モジュール6との間の取引を委託するためにも適用される(ステップ690～698)。これは発行銀行1からの電子マネーの1つの完全な引出しのための処理を完了する。

【0336】Aコルレスの銀行からの引出し

ここで、図44を参照して、コルレス銀行2からの引出しについて説明する。まず、引出しをセットする前述のステップ43～48が金銭出納モジュールB5との関連において金銭取引モジュールA4により試みられる。次に期間を設定するため、やはり前述したステップ190～258が用いられ、これにより金銭出納モジュールB5及びC5間の取引が開始される。期間が設定された後、対銀行アプリケーションB47は引出しに対応する会計取引を実行する(ステップ900、更には図13のステップ1参照)。

【0337】すでに確認した通り、金銭取引モジュール4が、発行銀行1及びコルレス銀行2のいずれかの銀行と相互関係にある限り、金銭取引モジュール4内にストアされたすべての電子手形11は取り除かれ、最新の証明を含む電子手形11と置換される。このオペレーションを実行するため、対取引アプリケーションB49は、金銭モジュール4内に手形11がストアされているか否かをチェックする(ステップ902～904)。もし手形が存在するならば、対銀行アプリケーションB47は、妥当な会計取引を(図13、ステップ2において示された会計手続参照)明示し(ステップ906)、かつ、金銭出納モジュールC5(発行銀行1に関連する)

からの預金要求を実行して置換されるべき手形を返還する。

【0338】次に、図57を参照して預金要求の実行について詳細に説明する。ここに、対出納アプリケーション34は、預金要求メッセージと、送られるべき預金額と、手形11が預金されるべき口座の口座番号及び口座プロフィールを送信する(ステップ920)。この情報はメッセージを送るためのステップ2~8を用いて金銭出納モジュール5に転送され、次いで、ステップ7041~7056(図49参照)が口座プロフィール及び口座番号を有効化するように実行される。

【0339】預金元が金銭取引モジュール4である場合、金銭出納モジュール5の対取引アプリケーション49が、金銭取引モジュール4に対し手形11の移転を進める待機状態にあるという承認票を送信する(ステップ924)。一方、預金を実行するものが別の金銭出納モジュール5であれば、その金銭出納モジュール5に承認票を発行するのは、対出納アプリケーション34である(ステップ926)。

【0340】いずれの場合においても、承認票はステップ2~8において概説された手続を用いて暗号化、及び送信され、これによって承認票は預金する金銭モジュール5の対出納アプリケーション34により受信される(ステップ928)。

【0341】図44に戻ると、手形11は一度預金要求が完了すれば、金銭出納モジュールB5から金銭出納モジュールC5に移転される。これには手形の移転について前述した図51、52におけるステップ750~770が用いられる。したがって、対銀行アプリケーション47は妥当な会計取引を明示し(図13、ステップ2参照)、この手形11の移転を反映する(ステップ908)。金銭出納モジュールC5において、対出納アプリケーション34は、メッセージを対出納アプリケーションB34に戻されたメッセージを送ることによりその預金を承認する。これには、ステップ2~8が用いられる。当然ながら、対銀行アプリケーションB47はここで金銭出納モジュールC5に対してなされた引出し要求を反映する会計取引を明示する。(ステップ914、及び図13のステップ3参照)。

【0342】すべての電子手形11が金銭取引モジュール4から取り除かれて、妥当な口座が保持された後、加入者の銀行口座から引き出されるように最初に要求された金額と、更新された電子手形11と置換されるために、金銭取引モジュール4から取り除かれた金額の双方を含む合計金額の引出しが要求される。

【0343】引出し要求は、前述した図30、31におけるプロセスステップ700~724を用いて金銭出納モジュールB5及びC5の間で実行される。金銭出納モジュールC5は、金銭発生モジュール6と取り引きして新たな電子マネーを引き出すと共に、その実行中におい

て図40、及び図41~43のプロセスステップ190~258を用いることにより2つのモジュール間における期間を設定する。

【0344】図53のプロセスステップ780~792を用いて金銭出納モジュールC5より金銭発生モジュール6から取り出すことが要求される電子手形11は、図51、52のステップ750~770を用いることにより、金銭発生モジュール6から金銭出納モジュールC5に移転される。

【0345】対銀行アプリケーションC47は、会計明示を実行する(ステップ916、更には図13のステップ4参照)。この後で、電子手形11はステップ750~770を用いることにより、金銭出納モジュールC5からB5に移転され、更にはステップ750~770を用いて金銭取引モジュールA4に移転される。

【0346】コルレス銀行2からの引出しを完了するために、各金銭モジュールはそれが対応するモジュールと共に、その直前に行った取引を委託しなければならない。このようにして、金銭取引モジュールA4は、図54のステップ690~698を用いて金銭出納モジュールB5に委託し、その後で更に金銭出納モジュールC5に委託する。最後に、金銭出納モジュールC5は同じプロセスステップ690~698を用いて金銭発生モジュール6に委託する。

【0347】発行銀行への預金

図55を図56と合わせて参照することにより、発行銀行1への預金の例を詳細に説明する。取引を開始するため、預金の設定は図56に示したプロセスステップを用いて実行されなければならない。

【0348】図56の頂部におけるステップ398において、加入者は銀行にいくらかの金銭を預金しようと設定する。金銭取引モジュール4へのルーチンにサイン記入を行った後(図32~33のステップ10~42を辿る)、対加入者アプリケーションA33は、加入者が所望の取引に向かうように促める(ステップ400)。

【0349】この例において、加入者は預金取引と預金されるべき金額、並びに電子マネーを預金すべき銀行及び口座番号を選択する(ステップ402)。他の何らかの手続を実行する前に、手形ディレクトリアアプリケーションA39は金銭モジュールが預金要求を支持するに十分な資金を収容しているか否かをチェックする(ステップ404)。

【0350】預金のために不十分な資金しか存在しなければ、対加入者アプリケーションA33は、加入者が新たな金額を選択するように勧め(ステップ410)、新たな金額が選択されなければ、期間管理手段A32は、加入者に対し取引は終了したこと告知する(ステップ414)。しかしながら、加入者が新たな金額を入力した場合(ステップ412)、プロセスフローはステップ404に戻り、ここで手形ディレクトリアアプリケーション

39は再び取引に十分な資金があるか否かをチェックする。

【0351】金銭モジュール内に適当な資金が存在するものとして、プロセスフローは図35～36のステップ50～168において概括されたネットワーク25のサインオン手続に移る。有効なネットワーク25のサインオンが行われれば、プロセスフローはステップ190～258に進み、ここで金銭取引モジュールA4と金銭出納モジュールB5との間に期間が設定される。

【0352】一度2つの金銭モジュール間で期間が設定されると、手続920～928において概括された預金要求ステップは、その要求を金銭取引モジュールA4から金銭出納モジュールB5に転送する段階に移る。対出納アプリケーションA34は、金銭モジュール内にストアされたすべての電子手形11を金銭出納モジュールB5に移転する(ステップ408)。これは2個の金銭モジュール間における電子手形11の移転について前述したステップ750～770を用いる。

【0353】図55を同じく参照して、対銀行アプリケーションB47は、預金された手形のための会計取引を保持する(ステップ418、及び図12、ステップ1参照)金銭出納モジュールB5において、対取引アプリケーション49はモジュールAにストアされ、次いで、金銭出納モジュールB5に移転された全手形11より預金額の方が少ないか否かをチェックする(ステップ420)。預金額が移転された手形11の総額より少なければ、更新された手形11を発生してそれを金銭取引モジュール4に転送しなければならない。

【0354】金銭取引モジュール4に収容されたすべての手形が預金される、すなわち、預金されるべき金額が電子手形11の総計より小さい場合、対取引アプリケーションB49は金銭モジュール間においてメッセージを送るためのステップ2～8を用いて金銭取引モジュール4に承認票を送る(ステップ428)。対出納アプリケーションA34は承認票を受信し(ステップ430)、ステップ690～698を開始して2つの金銭モジュール間における預金取引に関与する。

【0355】取り除かれた電子手形11が所望の預金額を上回る場合には、新たに更新された手形11が金銭取引モジュール4に返還されなければならない。これを達成するため、金銭出納モジュールB5の対銀行アプリケーションB47が妥当な会計取引を保持する(ステップ424、図12、ステップ2参照)。然る後、金銭出納モジュールB5は、プロセスステップ190～258を用いて、金銭発生モジュール6との間で期間を設定し、かつ、ステップ780～792を実行することにより、金銭取引モジュール4に返還されるべき金額の電子手形11を、金銭発生モジュール6から取得するように要求する。

【0356】電子手形11は、金銭発生モジュール6に

より発生し、ステップ750～770を用いて金銭出納モジュールB5に移転される。金銭出納モジュールB5の所有に帰す電子手形11と共に、それらはステップ750～770を用いて金銭取引モジュールA4に移転される。

【0357】金銭取引モジュールA4が電子手形11を受信した後、それはステップ690～698を用いることにより、金銭出納モジュールB5を金銭取引モジュールA4に委託することにより、取引を終了させなければならない。同じく、金銭出納モジュールB5は、同じステップ690～698を用いて金銭発生モジュール6に関与しなければならない。

【0358】Aコルレス銀行への預金

図58は、コルレス銀行における預金についてのプロセスフローを示している。コルレス銀行への預金において、ステップ398～414に記載された預金設定は、取引の第一段階において繰り返される。対取引アプリケーションB49は、この段階から預金が預金設定手続において回収された電子手形11の総額より低いかなかをチェックする(ステップ440)。

【0359】金銭取引モジュール4にストアされたすべての電子手形11が、預金されるべき手形11の金額に等しい場合、対取引アプリケーションB49は、金銭取引モジュール4に預金承認票を返送し、ステップ2～8を用いて金銭出納モジュールB5からのメッセージを金銭取引モジュールA4に送信する。

【0360】金銭取引モジュール4側において、対出納アプリケーション34は承認票を受信し(ステップ446)、更にステップ690～698を用いてその取引を金銭出納モジュールB5に関与させる。金銭取引モジュール4は、同じ動作を終了し、プロセスから除去される。預金の終了は、対銀行アプリケーション47によってなされるべき口座明示取引のために提供される(ステップ448)。図11のステップ1は、会計取引の場合である。

【0361】ここで、ステップ190～258を用いることにより、金銭出納モジュールB5及び同モジュールC5との間において期間が設定される。

【0362】金銭出納モジュールB5は、プロセスステップ780～792を用いて、金銭出納モジュールC5に対し預金実行要求を発する。対銀行アプリケーションB47はここで会計取引を明示する(ステップ450及び図11、ステップ2参照)。

【0363】手形11はここでコルレス銀行B2から発行銀行C1に移転される。これにはステップ750～770が用いられ、発行銀行C1は対応する会計取引を明示する(ステップ452、更に図11、ステップ2参照)。対出納アプリケーションC34は、ステップ2～8を用いることにより、金銭出納モジュールB5の対出納アプリケーション34に対し(図59、ステップ45

71

6)、ステップ2~8を用いて預金認証票を送出することにより応答する(ステップ454)。

【0364】ここで、再び預金は、それが早期に取り除かれた電子手形11の総額より少ないか否かをチェックされる。預金が電子手形11より少なくない場合、その引出しは図54のプロセスステップ690~698を用いて完了し、これによって金銭出納モジュールB5が同モジュールC5に参与する。

【0365】引き出される手形の総額より少ない預金要求は口座の更新を要求し(ステップ460、及び、図11のステップ3参照)、新たな手形11がすでに取得された付加的な手形11と置換される。したがって、プロセスステップ920~928を辿る金銭出納モジュールB5からの金銭出納モジュールC5への引出し要求は、これら新規の電子手形11を提供するために実行される。

【0366】金銭出納モジュールC5は、まず、プロセスステップ190~258を用い、金銭発生モジュール6との間で期間を設定しなければならない。新たな電子手形11は、金銭出納モジュールC5によりプロセスステップ780~792を辿って、金銭発生モジュール6から要求され、これは更に金銭モジュール間で手形11を移転するためのステップ750~770を用いて金銭出納モジュールC5に移転される。

【0367】この金銭出納モジュールC5への電子手形11の移転は、対銀行アプリケーションC47により、会計取引が明示されることを要求する(図60、ステップ462、及び図11、ステップ3参照)。

【0368】手形11は、この状態において発行銀行1の金銭出納モジュールC5からコルレス銀行2の金銭出納モジュールB5、及び金銭取引モジュール4に移る。これには手形11を移転するためのステップ750及び770が用いられる。その後で各金銭モジュールは、それが期間を設定した相手である金銭モジュールに委託しなければならない。かくして、金銭取引モジュールA4は、金銭出納モジュールB5に委託し、これに伴って金銭出納モジュールB5は金銭出納モジュールC5に委託し、このモジュールC5はまた、金銭発生モジュール6に委託する。これら3つの関連取引のすべては、前述したプロセスステップ690~698を用いるものである。

【0369】加入者から加入者への支払

図46は、好ましい実施例において、1つの金銭取引モジュール4から別のモジュールへの支払い取引のためのプロセスフローを示している。この例において、アリス(仮定の支払法人であり、同図において“A”で指示)が、ボブ(すなわち、仮定の受取法人であり、図46において“B”で指示)に対して、特定額の電子マネーの支払を同意するものとする(ステップ800)。アリス及びボブは、前述したプロセスステップ10~42を用

72

いて、彼らの各金銭取引モジュール4に対しサインオンする。アリスは対加入者アプリケーションA33を介して、彼の金銭取引モジュール4を支払いに向け(ステップ806及び810)、一方、ボブは彼の金銭取引モジュール4を作動させて対加入者アプリケーションB33が支払受領という標識を発行させるようにする(ステップ808及び812)。

【0370】ステップ814及び816において、アリスの金銭取引モジュール4及びボブの金銭取引モジュール4の、各期間管理手段32は互いの通信を確立する。この状態からいずれか2個の金銭モジュール間の取引について、前述したステップ190~258の通りに期間が設定される。

【0371】期間が設定されると、対加入者アプリケーション33は、加入者が移転を要求する支払額を入力するように勧め(ステップ818)、これが加入者に対して表示される。

【0372】アリスは、ボブに対して移転しようとする金額を入力する。支払/交換アプリケーションA35は、入力された金額を受信する(図46、ステップ820)。ダイブにより入力された金額(通貨または信用)は、ここで手形ディレクトリアアプリケーション39により金銭取引モジュール4にストアされた電子マネーの値の残高と比較され、取引を進めるに十分な資金が存在するかどうか判定される(ステップ822)。

【0373】もし、資金が不十分であれば、対加入者アプリケーションA33は、加入者に対して所望の取引を支持するに十分な資金が存在しないことを告知し(ステップ824~826)、かつ、加入者に対し再び新たな支払額とするように勧める(ステップ827)。もし、加入者が新たな金額の入力を望まなければ、取引中止プロセスステップ500~524が作動状態となり、2つの金銭取引モジュール4間における通信リンクを終了する。他方、新たに金額が入力されると、プロセスはステップ820に戻って再び十分な資金があるか否かをチェックする。

【0374】移転を処理するために十分な資金が、金銭取引モジュールA4にストアされているときは、支払/交換アプリケーションA35がボブの金銭取引モジュール4に移転額を表すメッセージを送信する(ステップ828)。これには図47のステップ2~8に記載された処理が用いられる。ここで、対加入者アプリケーションB33はその所有者に対し移転されるべき金額が彼に受け入れられるか否かを検証する(ステップ830)。すなわち、ボブは移転されるべき金額を受け入れるか拒絶するかを決定することができる(ステップ832)。もし、ボブが否定的な応答を発した場合、支払/交換アプリケーションB35は、ステップ2~8を用いて移転されるべき金額が不正確であるというメッセージを、金銭取引モジュールA4に返送し(ステップ834)、プロ

セスは再び図46のステップ826に戻ってアリスに対し新たな金額を入力するように勧める。

【0375】一方、ボブが肯定的応答を発すると(ステップ832)、支払/交換アプリケーションB35はステップ2~8を用いて金銭取引モジュールA4に承認票を送信する(ステップ835)。承認票が金銭取引モジュールA4に戻ると、支払/交換アプリケーションA35には、金銭取引モジュールB4により送信された承認票を受信するようにメッセージが伝達される(ステップ836)。

【0376】この承認票が受信されると、支払/交換アプリケーションA35は移転されるべき所望額を金銭ホルダー38に送り(ステップ838)、これによってステップ750~770による電子手形11の移転が行われる。移転が完了すると、2つの金銭取引モジュール4は前述したステップ690~698を用いて移転の委託を行わなければならない。2つの金銭取引モジュール間の通信リンクはここで終了する。

【0377】加入者対加入者の外国為替取引

図61を参照すると、2つの金銭取引モジュール4間における外国通貨の交換のためのプロセスフローが示されている。この例においては、アリス(すなわち、図61~62において“A”で指示した仮定の法人とする)がボブ(すなわち、図61~62において“B”で示した別の仮定の法人とする)との間でドルをポンドに交換することを同意したものである。彼らが同意した為替レートはドル対ポンド比率である(ステップ300)。

【0378】アリスは彼の金銭取引モジュール4にサインオンし(これには前述したステップ10~42が用いられる)、ボブは彼の金銭取引モジュール4にサインオンする(ステップ10~42を用いる)ことにより取引が開始される。その後で、加入者の金銭取引モジュール4における対加入者アプリケーション33は各利用者が取引の形式を選択するように勧める(ステップ302~303)。この例においては、アリス及びボブは前者のドルを後者のポンド交換することを同意したものである。

【0379】外国為替取引を要求することにより、期間管理手段A31は期間管理手段B31との通信リンクを開設し(ステップ306、307)、これによりステップ109~258を用いて2つの金銭モジュール間に期間が設定される。アリスはここで対加入者アプリケーションA33により所定金額のドルを売り、かつその取引において所定の為替レートを用いるように勧められる(ステップ208)。

【0380】支払/交換アプリケーションA35は入力を受信し(ステップ310)、手形ディレクトリアアプリケーションA39は要求された金額が金銭取引モジュール4中に収容された値の総額と比較することにより十分な資金が存在するか否かをチェックする(ステップ31

2)。資金が不十分な状態であれば、対加入者アプリケーションA33はアリスに対し資金不十分というメッセージを送り、加入者が先の入力と異なる金額のドル及び為替レートを選択するように勧める(ステップ318~320)。新たな選択が入力されると、プロセスフローはステップ312に復帰してそこからのシーケンス動作を続行する。アリスが新たな金額を選択しなければ、取引中止ステップ500~524を用いて期間を消滅させる。

10 【0381】資金が要求された金額に見合う適当量であれば、支払/交換アプリケーションA35はその金額のドル及び提示されたドル/ポンド交換レート(ステップ316)をステップ2~8(図62参照)を用いて金銭取引モジュールB4の対加入者アプリケーション33に送信する。この点において、対加入者アプリケーションB33はボブに対しアリスが提示した金額及びレートを知らせ、その値はボブが交換に同意するものであるか否かを判定する(ステップ322)。

【0382】支払/交換アプリケーションB35がアリスによって提示されたドル金額及びレートを受入れ、しかも、その金額及びレートにボブが同意しなければ、支払/交換アプリケーションB35は金銭価値又は為替レートが不正確であることを支持するメッセージを送る(ステップ326)。これはメッセージ送信のためのステップ2~8を通じて行われる。対加入者アプリケーションA33はアリスがもう一度ドル金額及び為替レートを提示するように勧める(ステップ327)。新たな値が入力されると、プロセスは図61を参照してステップ310に戻り、新たな値が入力されなければ、取引中止プロセスステップ500~524が開始される。

【0383】金額及びレートがボブにより同意されると、支払/交換アプリケーションB35は提示されたレートに基づき(図示せず)同額のポンドを計算し、さらに、手形誘導アプリケーションB39を含むステップを開始して金銭取引モジュールB4が為替取引を満足するに十分な資金を収容しているか否かをチェックする(ステップ323)。金銭取引モジュールB4中の資金が為替取引に適合するには不十分であるとき、支払/交換アプリケーションB35はステップ2~8を用いてアリスに対して資金が不十分である(ステップ325)というメッセージを送信する。ここで、プロセスフローはステップ327に復帰する。

【0384】金銭取引モジュールB4中に十分な資金が存在する場合、支払/交換アプリケーションB35はステップ2~8を用いて金銭取引モジュールA4に承認票を送る(ステップ329)。この承認票が受信された後、支払/交換アプリケーションA35は要求されたドル金額をステップ330において対応する金銭ホルダーアプリケーション38に送信する。ドルは手形11を移転することについて前述したステップ750~770を介

75

してアリスからボブに移転される。

【0385】支払／交換アプリケーションB35は手形11を受け取り、その金銭ホルダアプリケーション38にその金額のボンドを転送する(ステップ331)。電子ボンドはここからステップ750～770において説明された手形移転プロセスを用いてアリスに移転される。この為替取引を記録するため、金銭取引モジュールA4は上述したプロセスステップ690～698を用いて金銭取引モジュールB4に委託する。満足な為替取引が行われると、2つの金銭取引モジュール間の通信リンクはここで終了する。

【0386】発行銀行における外国為替取引
ここで図65を参照すると、加入者が他の加入者との間ではなく、発行銀行1との間で彼のドルをボンドに交換した場合についてのプロセスが示されている。

【0387】加入者Aは上述したステップ10～42を用いて、彼の金銭取引モジュール4にサインオン(図63参照)することにより外国為替取引を明示する。対加入者アプリケーションA33は加入者が所望の取引を提示するようにすすめる(ステップ334)、この場合、加入者はドル／ボンド交換、及び交換すべきドル金額を選択する。銀行が取引するという選択は任意事項として加入者に提示される(ステップ336)。

【0388】手形ディレクトリアアプリケーションA39は要求を満足するに十分な残高が存在するか否かをチェックする(ステップ388)。残高が不十分であれば、加入者は再び彼が交換を望む金額を入力し(ステップ340～342)、これにより期間管理手段A31は新たな金額が提示されなければ、取引を終了する(ステップ345)。新たな金額が入力されると、プロセスはステップ388に復帰して新たな要求に適合する十分な資金があるか否かをチェックする。資金が交換要求のために十分であれば、ステップ50～168を用いたネットワーク25の動作を開始する。

【0389】ネットワーク25のサインオン、すなわち活用段階に入ると、ネットワーク25は銀行又は金融機関が選択されたか否かをチェックする(ステップ346)。最初に、銀行又は金融機関が選択されていなければ、対出納アプリケーションA34はネットワークサービス手段26に期間管理手段A32を用いて為替取引を行う銀行又は金融機関のリストを提示しなければならない(ステップ348～350)。ネットワークサービス手段26はそのリストを(レートとともに)対出納アプリケーションA34及び対加入者アプリケーションA33を介して加入者に送信する(ステップ352～356)。

【0390】提示された後(図64、ステップ367)、加入者は銀行もしくは金融機関を選択するか、又は取引を終了する(ステップ759)。銀行又は金融機関が選択されると、前述したステップ190～258を

76

用いて選択された金銭出納モジュール5との間で期間が設定される。期間が設定された後、対出納アプリケーションA34はメッセージの暗号化及び送信に関するステップ2～8を用いてボンドに交換(ステップ360)されるべきドル金額を送信する。

【0391】加入者が為替取引を進めることをなお望んでいることを確認するため、対取引アプリケーションB49はプロセスステップ2～8を用いて加入者に最新の交換レートを送信する(ステップ362)。この点において、対加入者アプリケーションA33は加入者が銀行の交換レートを知り、もし交換処理を望まなければ、次のステップ500～524により取引が中止される(ステップ364～366)。取引が進められる場合、ドルは金銭取引モジュールA4から金銭出納モジュールB5に移転されるが、これにはステップ750～770が用いられる。

【0392】図65を参照して、ひとたび外国為替取引の設定が行われれば、妥当な会計取引が明示され(ステップ368、図15のステップ参照)、移転された直後のドルを反映する。金銭出納モジュールB5と金銭発生モジュール6との間には、ステップ190～258を介して期間が設定される。金銭出納モジュールB5はプロセスステップ780～792を介して妥当な金額のボンド手形11を要求する。手形11は金銭発生モジュール6から金銭出納モジュールB5に戻され、これにはステップ750～770が用いられる。

【0393】この後者の態様における手形11の移転は、これに伴う口座の対応する更新を要求する(ステップ370、図15のステップ2参照)。手形11はプロセスステップ750～770を介して金銭取引モジュールA4に移転される。交換を完了すると、金銭取引モジュールA4はステップ690～698を用いて金銭出納モジュールB5に閏与し、その結果、このモジュールB5は金銭発生モジュール6に閏与する。

【0394】Aコルレス銀行における外国為替取引
コルレス銀行2との外国為替取引については、図66を参照して説明する。まず、ステップ334～366(図63～64)を繰返すことにより、外国為替取引が明示されるとともに、適当な口座が更新されて(図16のステップ1～2参照)、加入者の金銭モジュール4から金銭出納モジュールB5に移転された直後の手形11を反映する(ステップ372)。しかる後、金銭出納モジュールB5はプロセスステップ190～258を実行することにより、発行銀行1における金銭出納モジュールC5との間で期間を設定する。

【0395】前述したプロセスステップ920～928を用いて金銭出納モジュールB5により金銭出納モジュールC5に対して引出要求が発せられる。要求された手形11を獲得するため、金銭出納モジュールC5はそれらを金銭発生モジュール6から得なければならない。し

77

たがって、2つの金銭モジュール間にはステップ190～258を介して期間が設定されるとともに、先に概括されたプロセスステップ780～792を辿って手形11が要求される。

【0396】金銭発行モジュール6は要求された手形11を発生し、それらをプロセスステップ750～770により金銭出納モジュールC5に移転する。これに続き、銀行Cのシステムにおける適当な口座に対する転記が行われる(ステップ374及び会計取引のための図16のステップ3参照)。手形11はここで金銭出納モジュールC5から金銭出納モジュールB5を介して金銭取引モジュールA4に移転される。各移転のためには、プロセスステップ750～770が用いられる。最後に、すべての期間(セッション)が委託されなければならない。すなわち、金銭取引モジュールA4は金銭出納モジュールB5に委託し、このモジュールB5はステップ690～698を用いて金銭出納モジュールC5に委託する。金銭出納モジュールC5は金銭発生モジュール6に関連してドルからポンドへの交換を完了させる。

【0397】手形の更新、証明

すでに述べた通り、手形の満期日は安全機能として用いられ、これは満了するまで金銭取引モジュール4にストアされる。もし満了すると、その手形11の所持者はそれらを別の金銭取引モジュール4に移転することはできないが、参加銀行又は金融機関との取引によりそれらを預金もしくは新たな手形に交換することができる。

【0398】さらに、特定の金銭取引モジュール4に関する証明が消滅すると、加入者はネットワーク25をサインオンしてその証明を別の金銭モジュールとの取引のために更新しなければならない。以下の説明は、消滅した証明又は満了した手形11を更新するためのプロセスフローに関するものである。

【0399】図67の頂部において、加入者は前述したステップ10～42を用いて金銭取引モジュール4をサインオンし、対加入者アプリケーションA33によって取引を選択するように勧められる(ステップ570)。“更新”処理を選択した後、ネットワーク25の利用はステップ50～168を用いて実行される。ネットワーク25へのサインオンは証明の更新を実行する。これは図35～36を参照してすでに述べた通りである。

【0400】手形11を更新するため、期間管理手段A31はネットワーク25に手形更新要求を送信する(ステップ574)。ネットワークサービス手段26はこれに回答して金銭取引モジュール4に選択された銀行の認識番号を返送する(ステップ576)。ここで、ステップ190～258を用いて金銭取引モジュールA4と選択された銀行の金銭出納モジュールB5との間に期間が設定される。

【0401】ひとたび期間が設定されると、対出納アプリケーションA34はステップ2～8におけるメッセー

78

ジ送信ルーチンを用いて手形11を更新する(ステップ578)要求を送る。対取引アプリケーションB32はこれに回答して図68に示すように、ステップ2～8を用いて送られた承認票(ステップ580)を有する。ここで、金銭取引モジュールA4はステップ750～770を用いて金銭出納モジュールB5に満了した手形11を転送することができる。対応する会計(図24のステップ1参照)がこの後で銀行のレコードにおいて実行され(ステップ582)、ステップ190～258を介して金銭出納モジュールB5と金銭発生モジュール6間に期間が設定される。

【0402】ステップ780～792の手形要求ルーチンが次いで実行される。金銭発行モジュール6はステップ750～770を介して要求された手形11を送るとともに、銀行口座を更新する(ステップ584、図24のステップ2参照)。金銭出納モジュールB5は更新された手形11を取得し、それらを同じステップ750～770を用いて金銭取引モジュールA4に送る。

【0403】ここで、手形11が金銭取引モジュール4において更新されたということであり、期間は金銭取引モジュールA4が金銭出納モジュールB5に委託し、かつ金銭出納モジュールB5が金銭発生モジュールによる取引を委託することにより完了する。最後に、2つの委託ルーチンは前述したステップ690～698を用いて実行される。

【0404】前述したプロセスフローは、経済的価値の電子的象徴を為替取引するための改良されたシステムを提供する本発明の能力を示すものである。それは紙幣本意の通貨システムによる固有の制約を排除するものである。

【0405】本発明の動作は基本的には、同一プロセスにおいて加入者により利用される通貨手形及び信用手形について説明されたものである。そのシステムはまた、他の通貨制度に適用することも可能である。例えば、個人及び法人小切手及び銀行為替手形の取引適用性を拡大することが可能であり、信用上及び銀行の受取手形のようにより複雑な多部門の支払プロセスについてもシステムに適当な変形を加えて適用することができる。本発明のシステムはまた、商業手形などのような法人の金融債務を提供するためにも適用することができる。

【図面の簡単な説明】

【図1】本発明の概要を示す線図である。

【図2】本発明による構成要素の機能的配列を示す略図である。

【図3】本発明による金銭モジュールを收容した外部システムの幾つかの実施例を示す斜視図である。

【図4】本発明による金銭取引モジュールのブロック線図である。

【図5】本発明による金銭出納モジュールのブロック線図である。

【図6】本発明による金銭発生モジュールのブロック線図である。

【図7】本発明によるネットワーク構成を示すブロック線図である。

【図8】本発明によるネットワークサービス手段のブロック線図である。

【図9】本発明による安全保障システムのブロック線図である。

【図10】本発明による安全保持手段のブロック線図である。

【図11】本発明による会計例を示すフロー線図である。

【図12】本発明による会計例を示すフロー線図である。

【図13】本発明による会計例を示すフロー線図である。

【図14】本発明による会計例を示すフロー線図である。

【図15】本発明による会計例を示すフロー線図である。

【図16】本発明による会計例を示すフロー線図である。

【図17】本発明による会計例を示すフロー線図である。

【図18】本発明による会計例を示すフロー線図である。

【図19】本発明による会計例を示すフロー線図である。

【図20】本発明による会計例を示すフロー線図である。

【図21】本発明による会計例を示すフロー線図である。

【図22】本発明による会計例を示すフロー線図である。

【図23】本発明による会計例を示すフロー線図である。

【図24】本発明による会計例を示すフロー線図である。

【図25】本発明による取引調整システムのフロー線図である。

【図26】本発明による決済システムのフロー線図である。

【図27】本発明による金銭発行調整システムのフロー線図である。

【図28】本発明による取引例を示すフローチャートである。

【図29】本発明による取引例を示すフローチャートである。

【図30】本発明による取引例を示すフローチャートである。

【図31】本発明による取引例を示すフローチャートである。

【図32】本発明による取引例を示すフローチャートである。

【図33】本発明による取引例を示すフローチャートである。

【図34】本発明による取引例を示すフローチャートである。

10 【図35】本発明による取引例を示すフローチャートである。

【図36】本発明による取引例を示すフローチャートである。

【図37】本発明による取引例を示すフローチャートである。

【図38】本発明による取引例を示すフローチャートである。

【図39】本発明による取引例を示すフローチャートである。

20 【図40】本発明による取引例を示すフローチャートである。

【図41】本発明による取引例を示すフローチャートである。

【図42】本発明による取引例を示すフローチャートである。

【図43】本発明による取引例を示すフローチャートである。

【図44】本発明による取引例を示すフローチャートである。

30 【図45】本発明による取引例を示すフローチャートである。

【図46】本発明による取引例を示すフローチャートである。

【図47】本発明による取引例を示すフローチャートである。

【図48】本発明による取引例を示すフローチャートである。

【図49】本発明による取引例を示すフローチャートである。

40 【図50】本発明による取引例を示すフローチャートである。

【図51】本発明による取引例を示すフローチャートである。

【図52】本発明による取引例を示すフローチャートである。

【図53】本発明による取引例を示すフローチャートである。

【図54】本発明による取引例を示すフローチャートである。

50 【図55】本発明による取引例を示すフローチャートである。

81

【図56】本発明による取引例を示すフローチャートである。

【図57】本発明による取引例を示すフローチャートである。

【図58】本発明による取引例を示すフローチャートである。

【図59】本発明による取引例を示すフローチャートである。

【図60】本発明による取引例を示すフローチャートである。

【図61】本発明による取引例を示すフローチャートである。

【図62】本発明による取引例を示すフローチャートである。

【図63】本発明による取引例を示すフローチャートである。

【図64】本発明による取引例を示すフローチャートである。

【図65】本発明による取引例を示すフローチャートである。

【図66】本発明による取引例を示すフローチャートである。

82

ある。

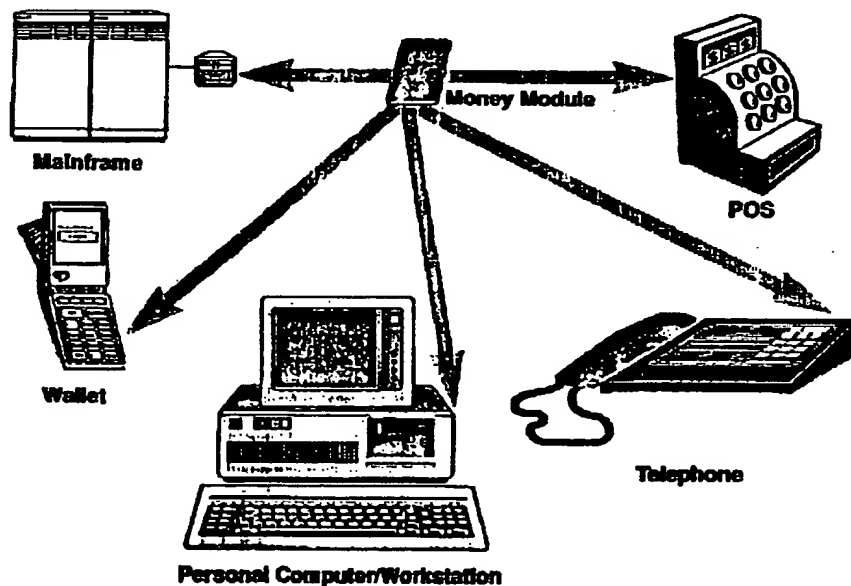
【図67】本発明による取引例を示すフローチャートである。

【図68】本発明による取引例を示すフローチャートである。

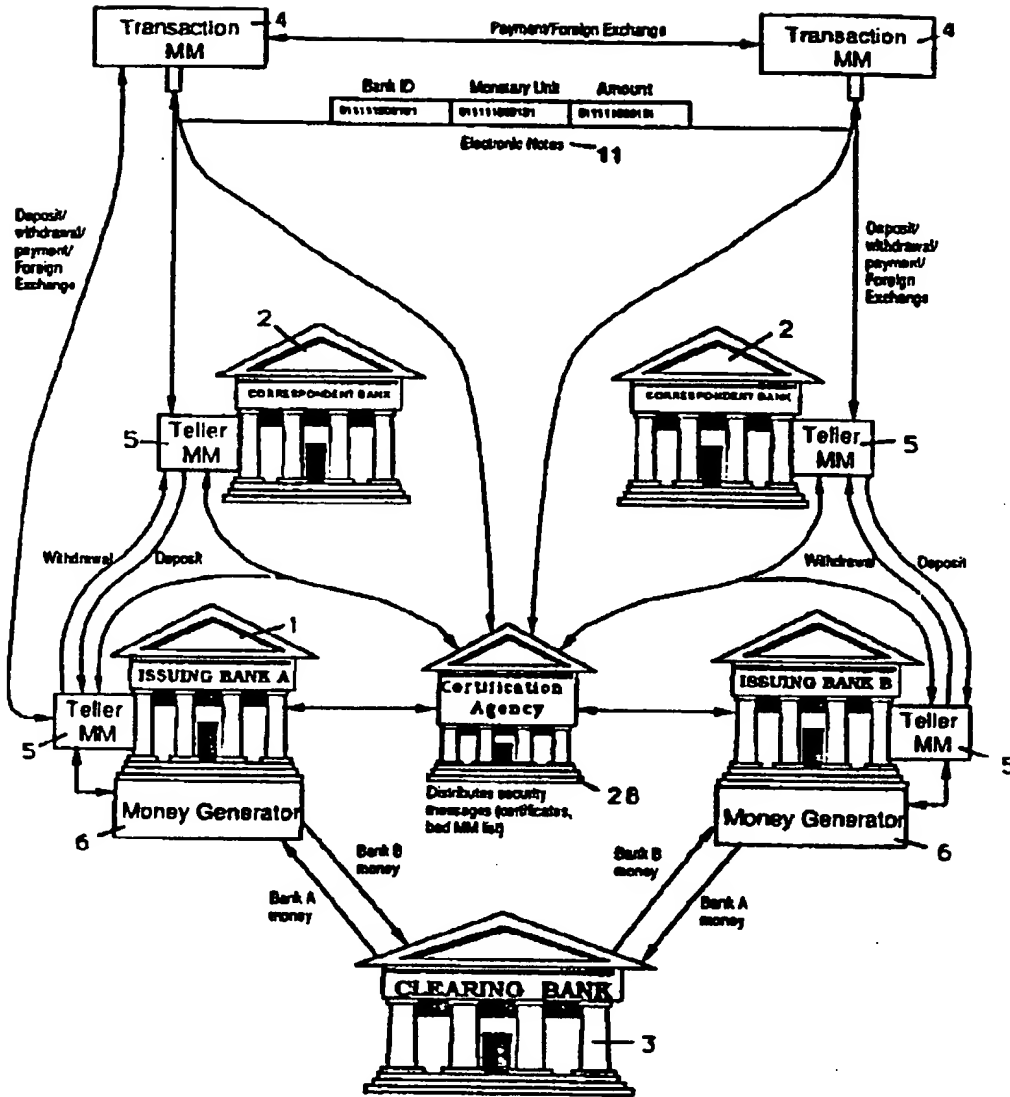
【符号の説明】

- 1 発行銀行
- 2 コルレス銀行
- 3 決済銀行
- 10 4 金銭取引モジュール
- 5 金銭出納モジュール
- 6 金銭発生モジュール
- 11 電子手形
- 13 決済システム
- 20 銀行体系
- 21 安全保障システム
- 22 取引調整システム
- 23 金銭発行調整システム
- 24 金融状態システム
- 20 28 証明機関

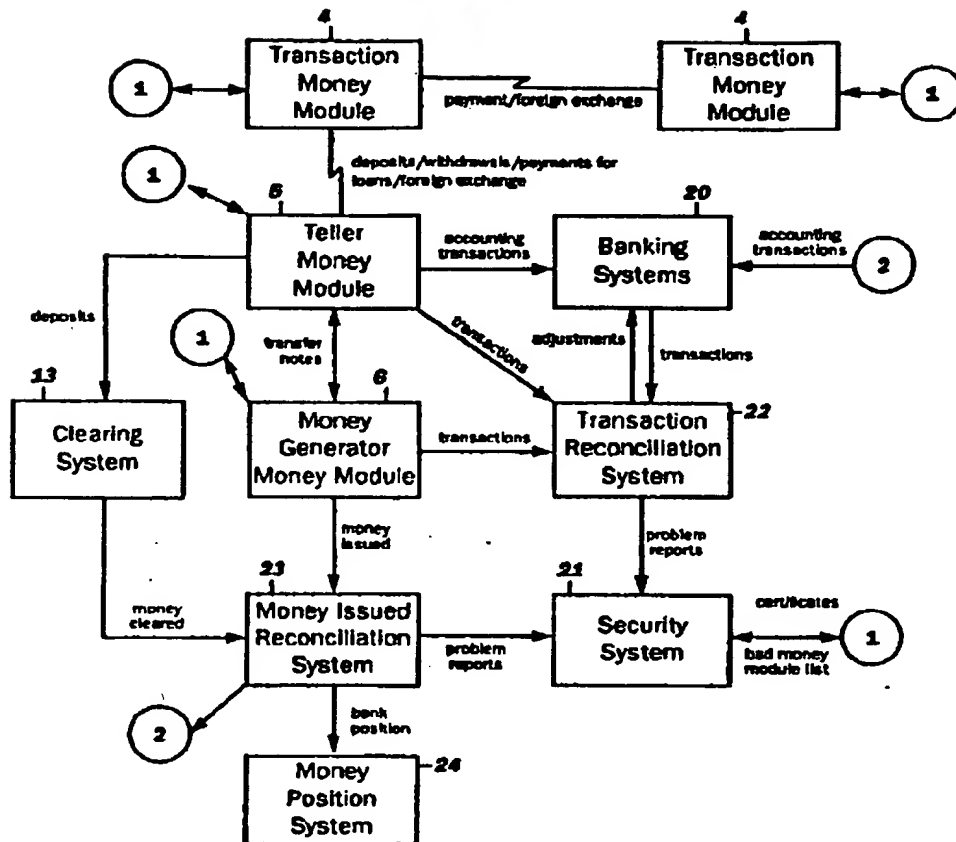
【図3】



【図1】



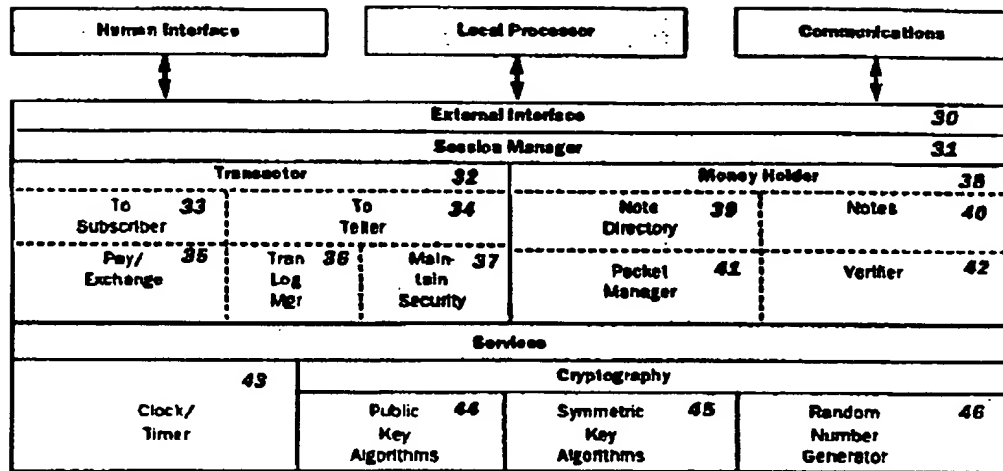
【図2】



Network 25 (not shown)

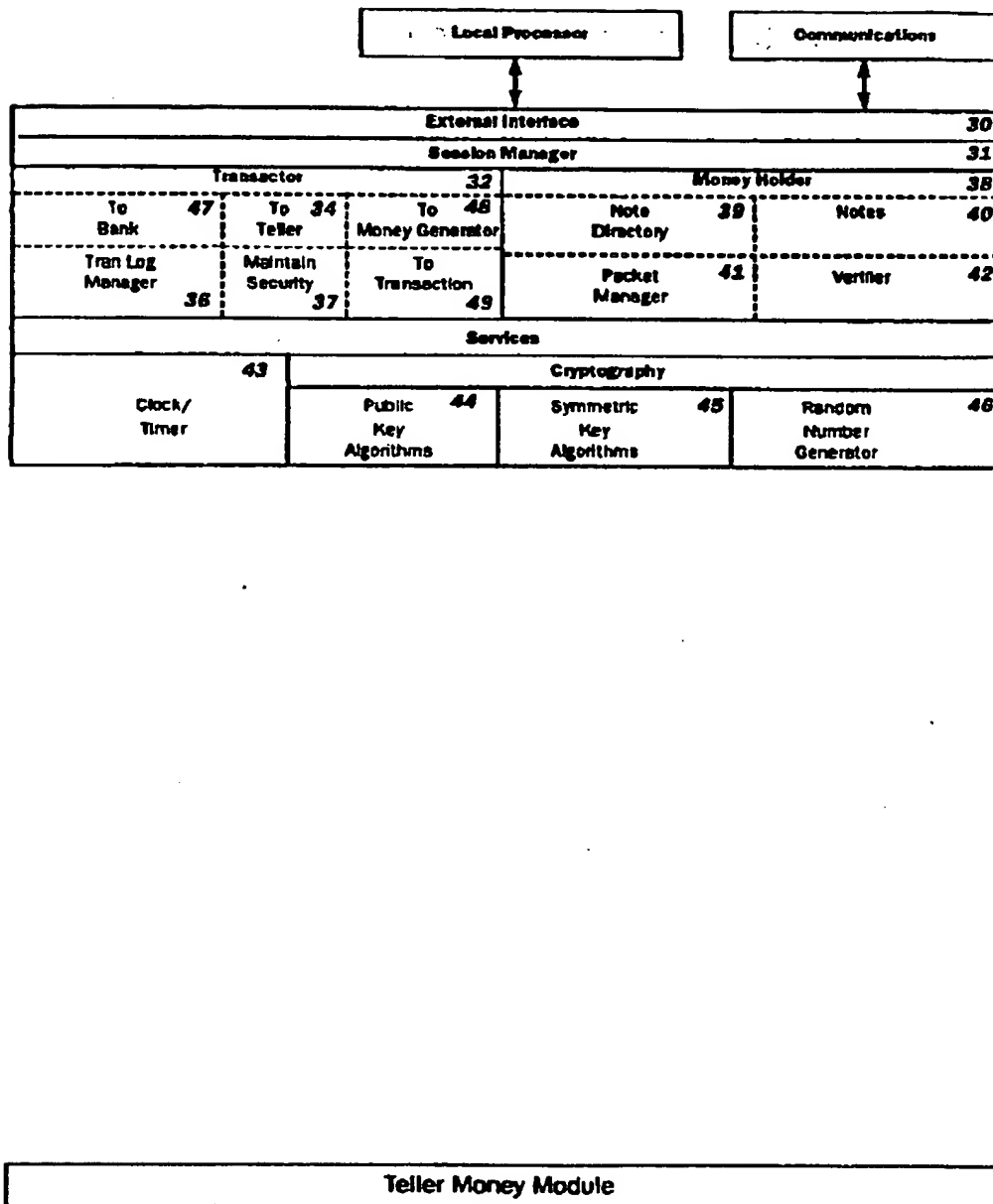
Electronic Monetary System

【図4】

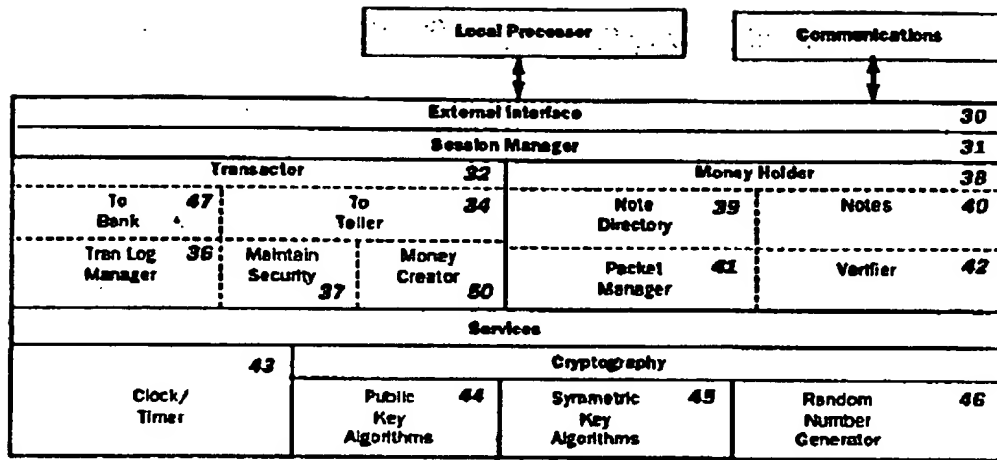


Transaction Money Module

【図5】

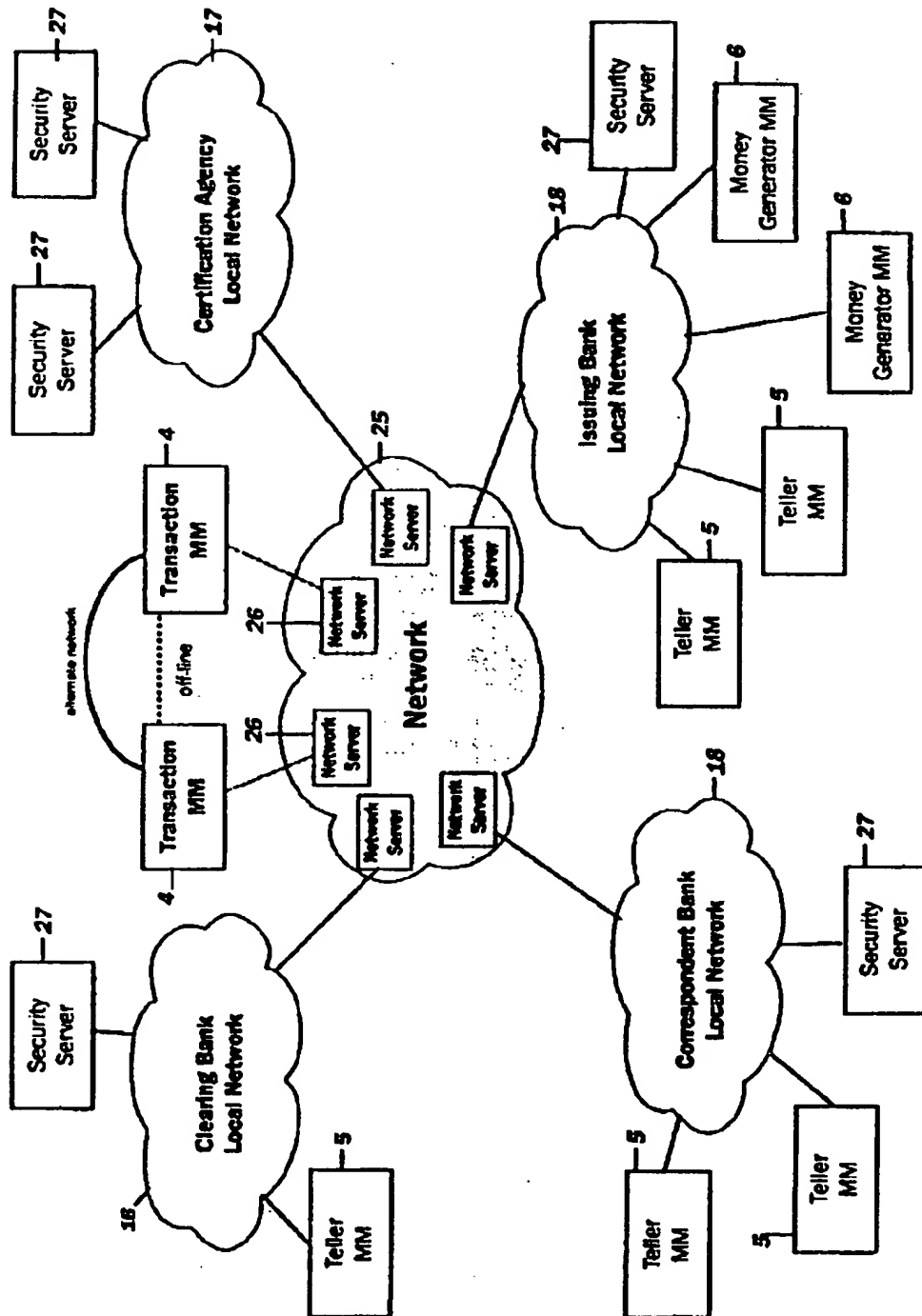


【図6】



Money Generator Module

【図7】

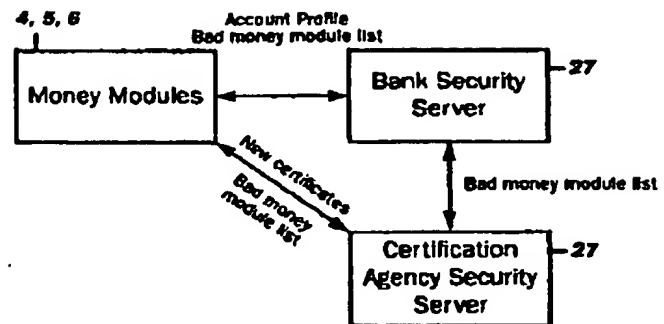


【図8】

External Interface				56
Communication Session Manager				57
Application Services				
58	Manage Network Sign-on	59	Synchronize Time/ date	Route Message 60
				Direct to Bank Service 61

Network Server

【図9】



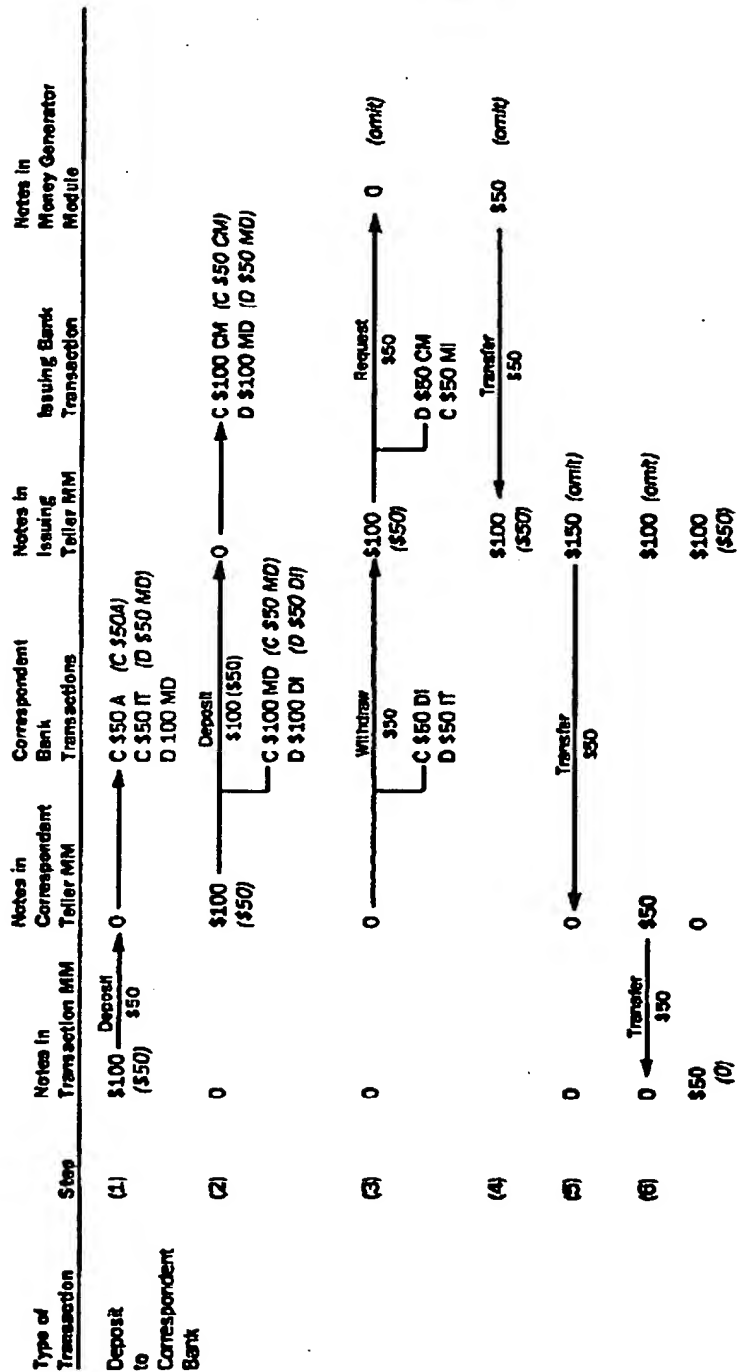
Security System

【図10】

External Interface				54
Session Manager				55
Create Certificate	50	Create Account Profile	51	Distribute Certification Keys
				52
				Control Bad Money Module Lost
				53
Services				
Clock/ Timer	43	Cryptography		
		Public Key Algorithms	Symmetric Key Algorithms	Random Number Generator
		44	45	46

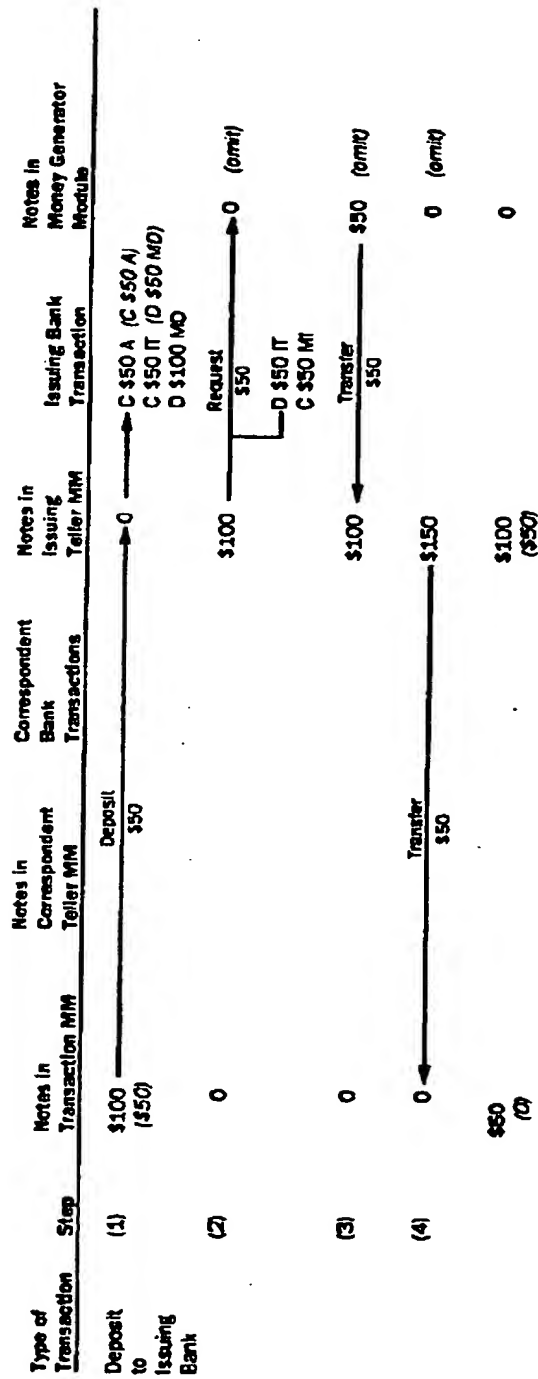
Security Server

【図11】



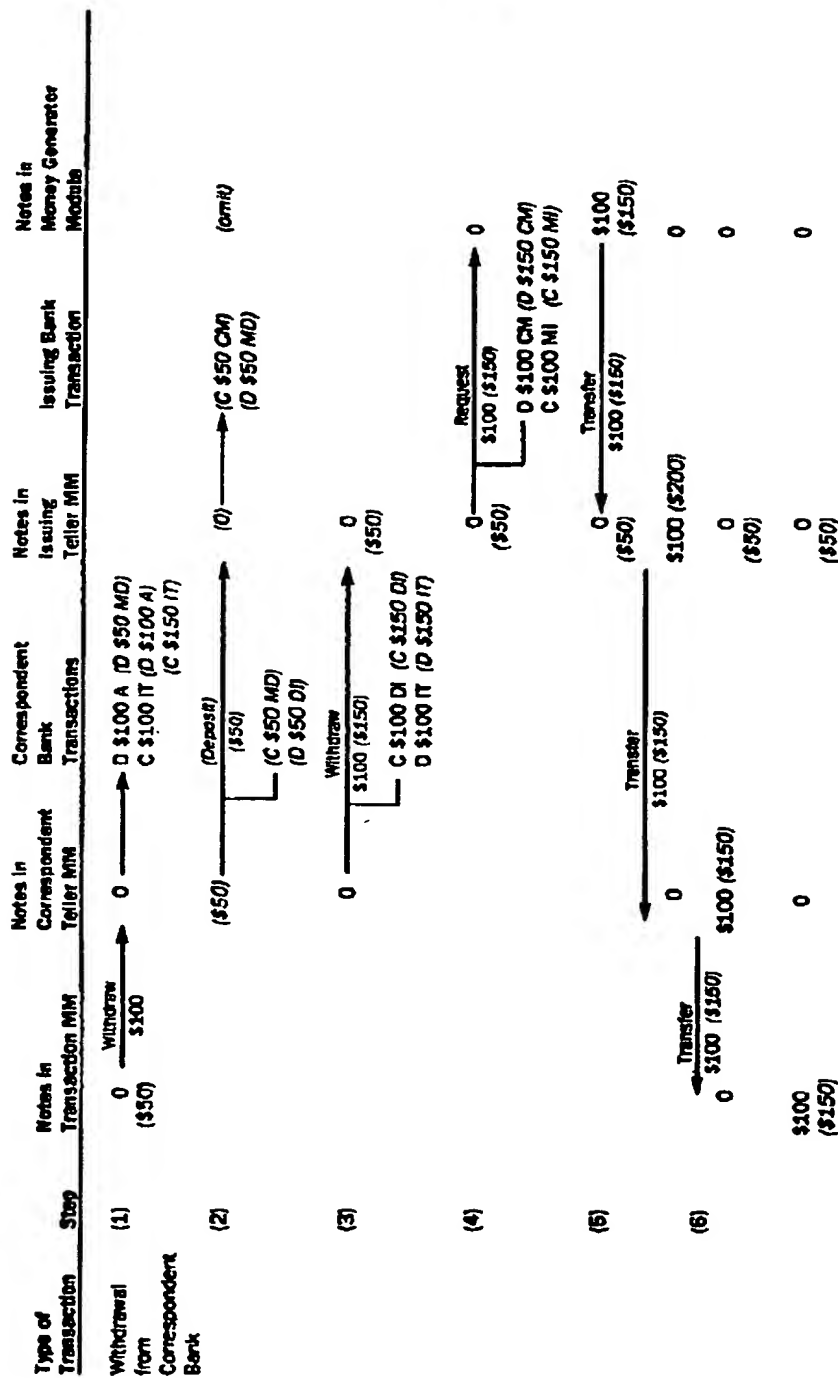
Key: () — Alternate values and steps

【図12】



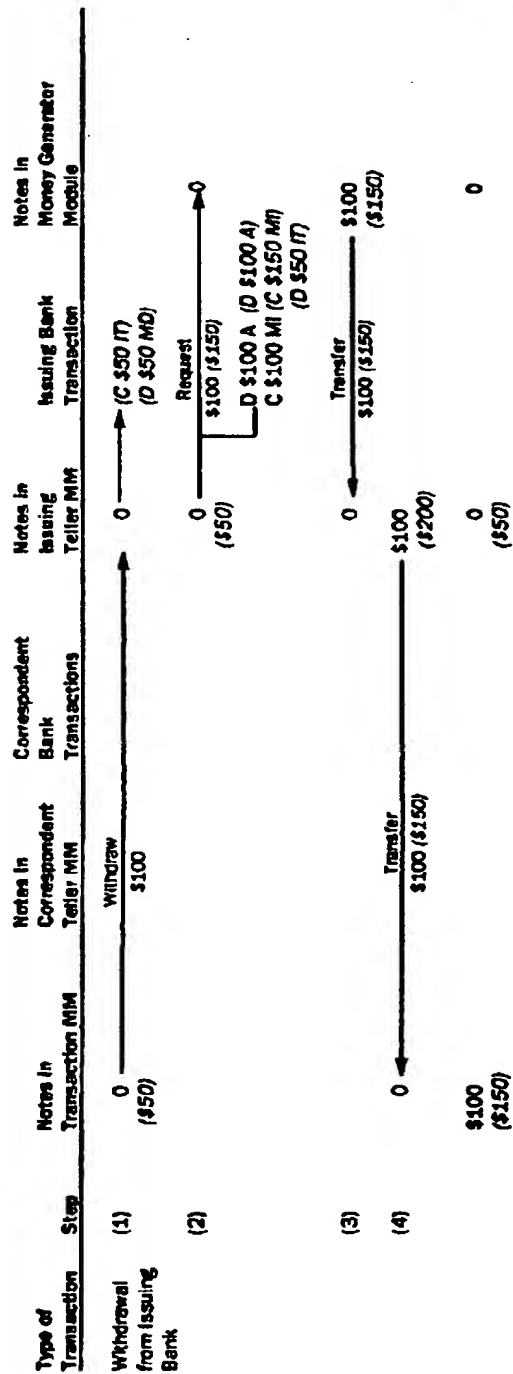
Key: () — Alternate values and steps

【図13】



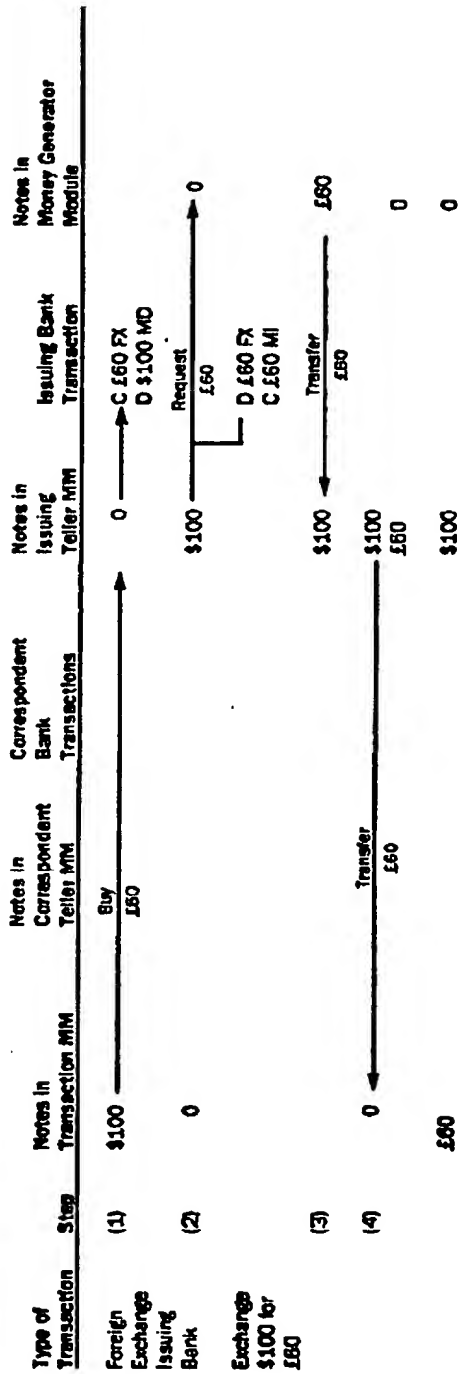
Key: () — Alternate values and steps

【 図 1 4 】



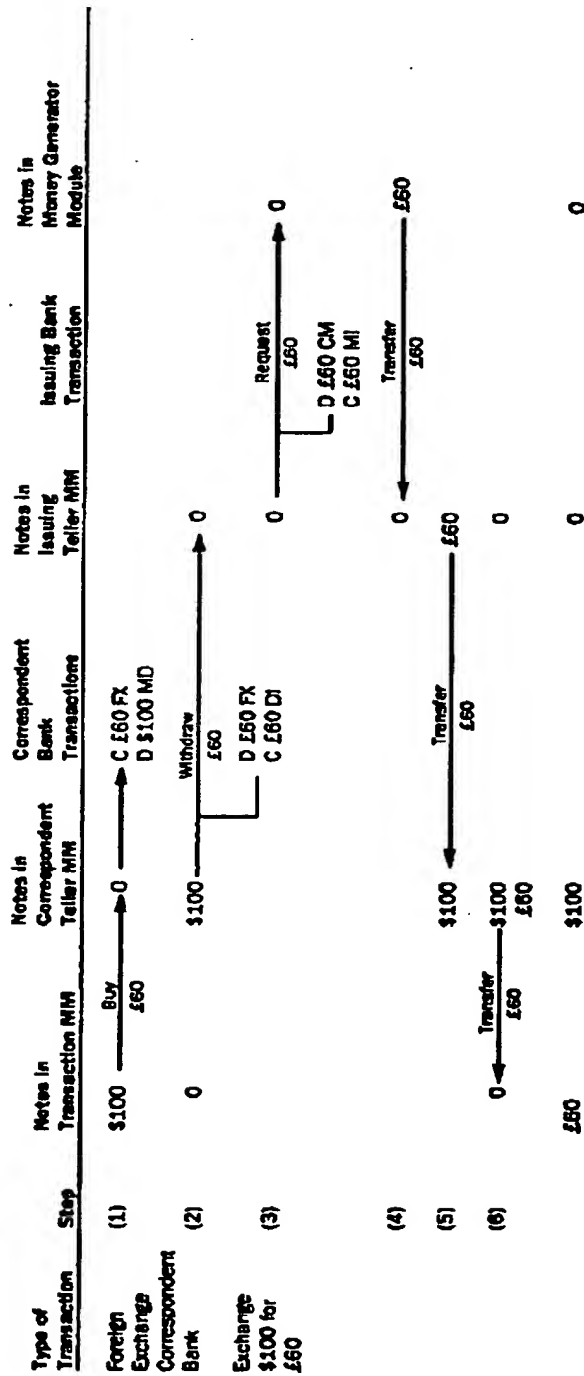
Key: () — Alternate values and steps

【図15】



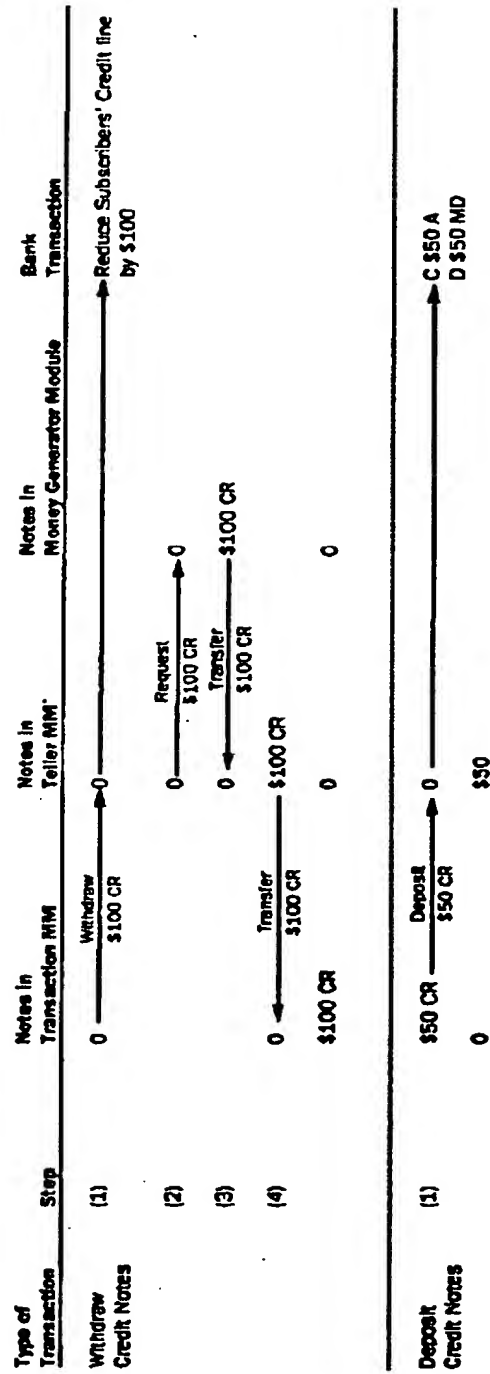
Key: () — Alternate values and steps

【図16】



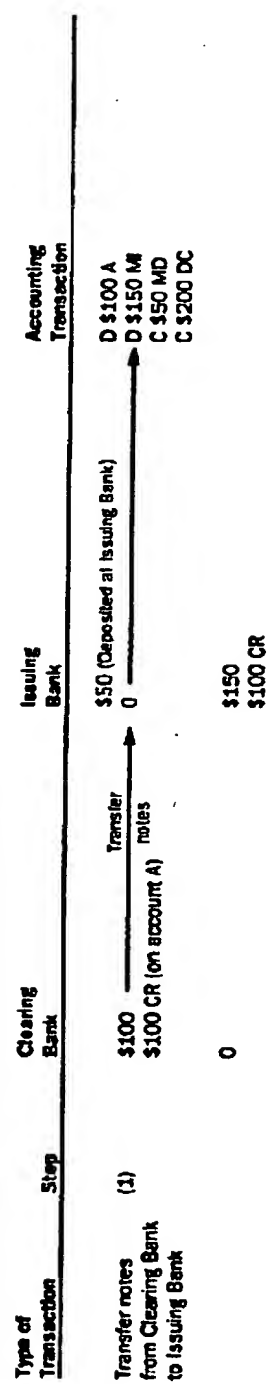
Key: () — Alternate values and steps

【図17】



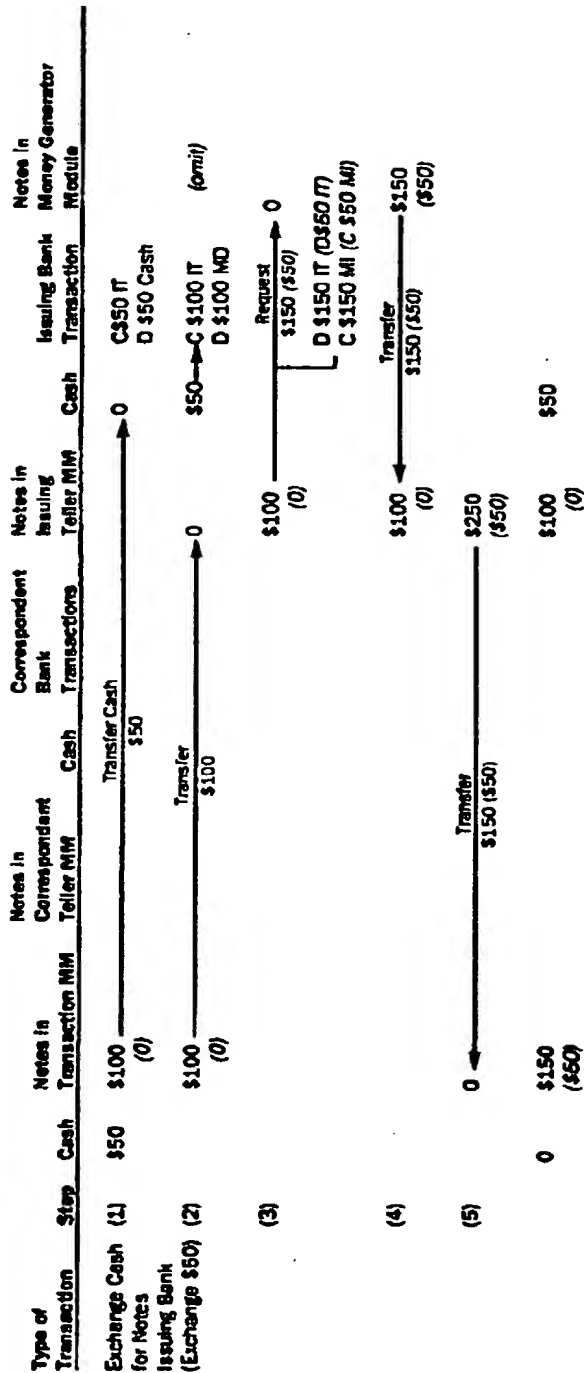
Key: () — Alternate values and steps

【図18】



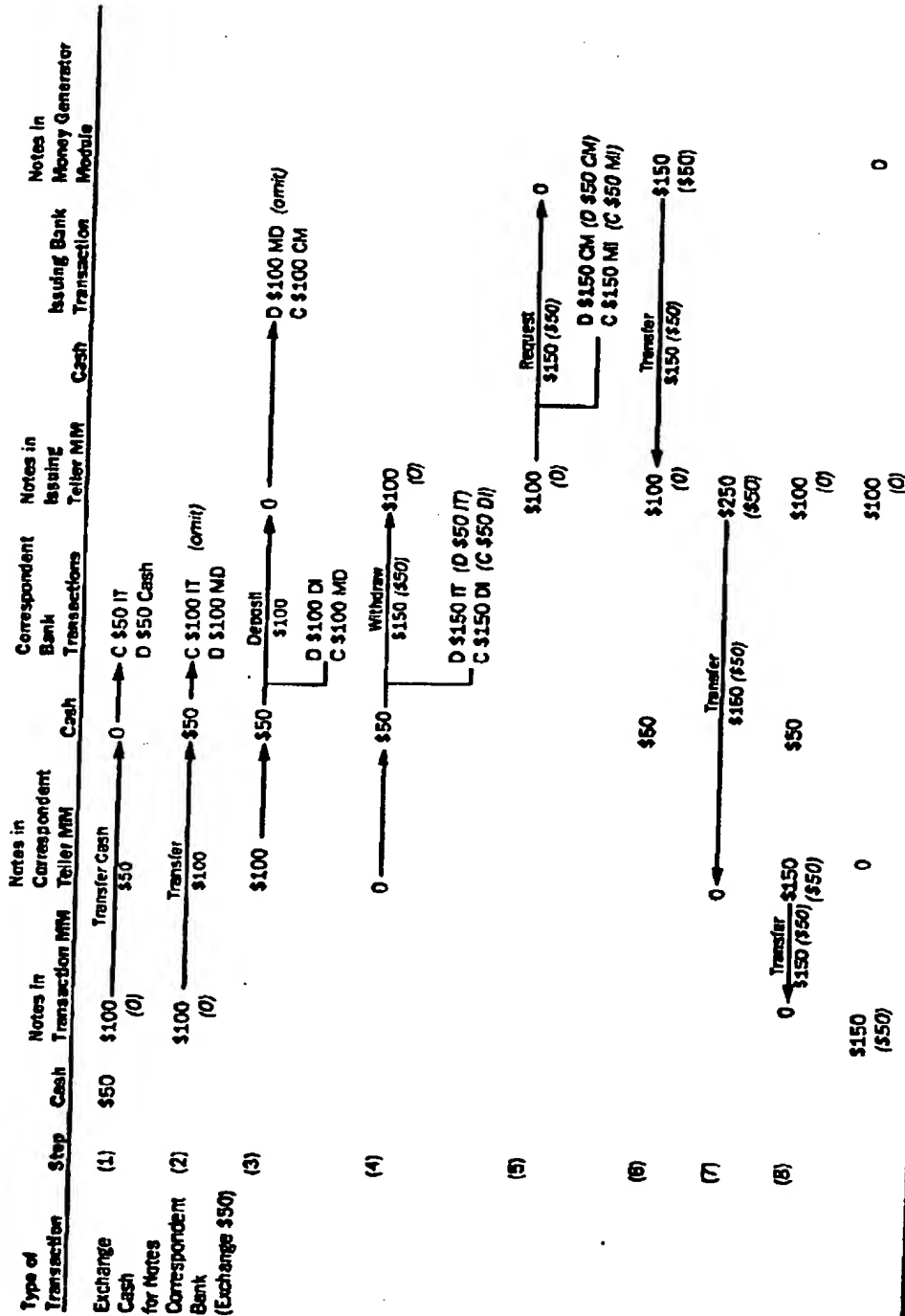
Key: () — Alternate values and steps

【図19】

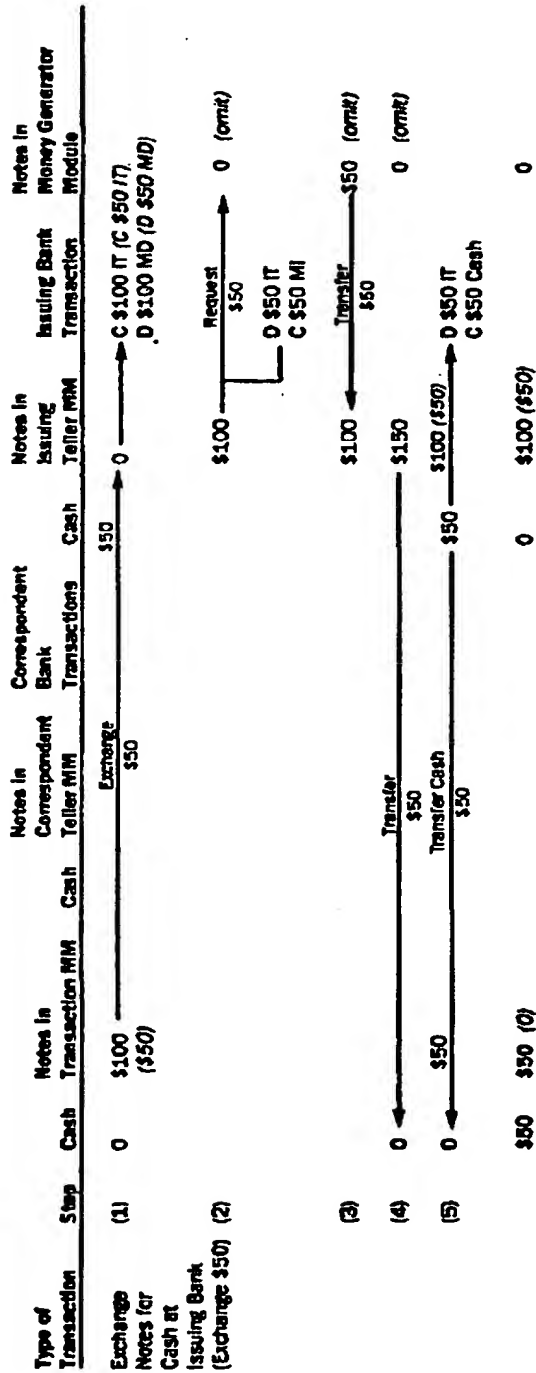


Key: () — Alternate values and steps

【図20】

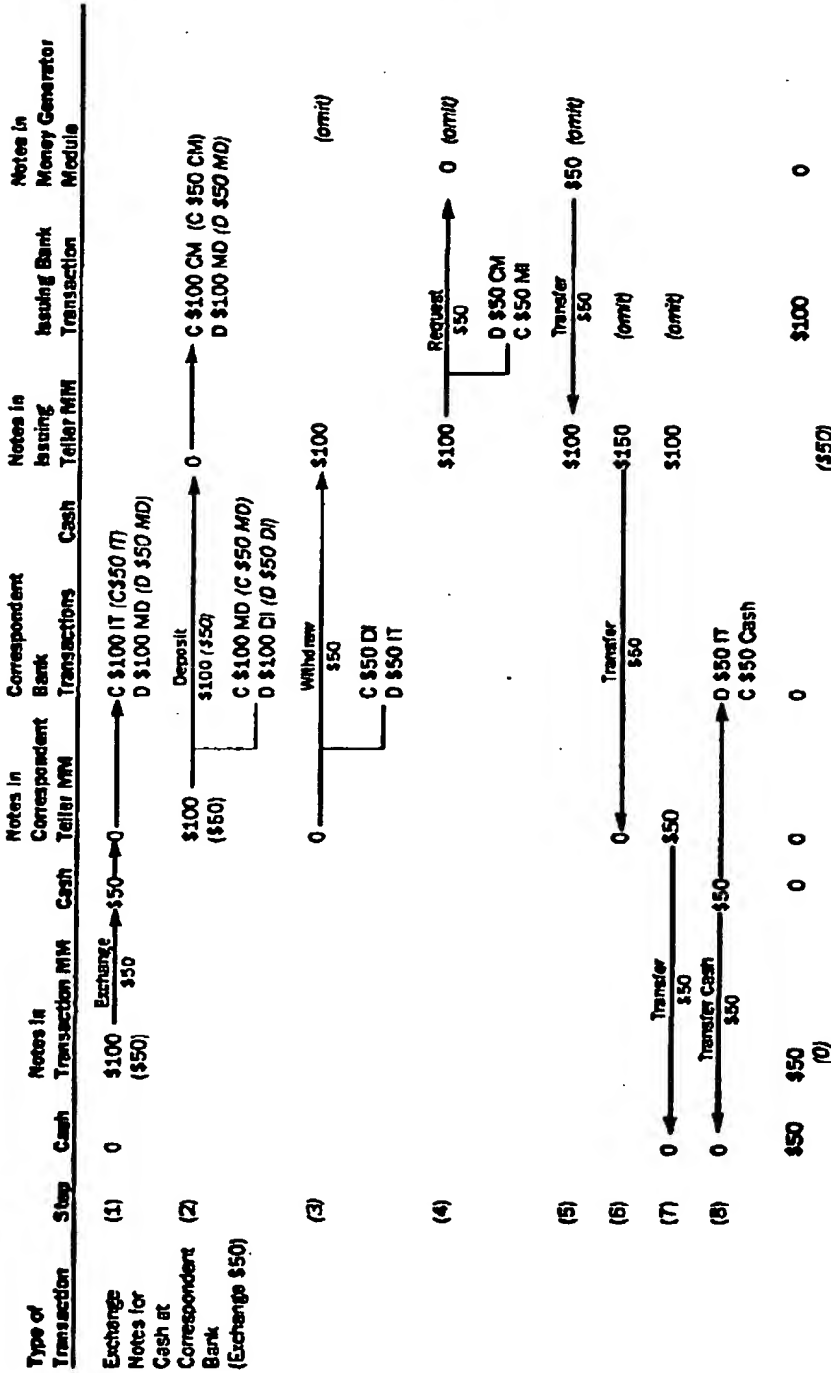


【図21】



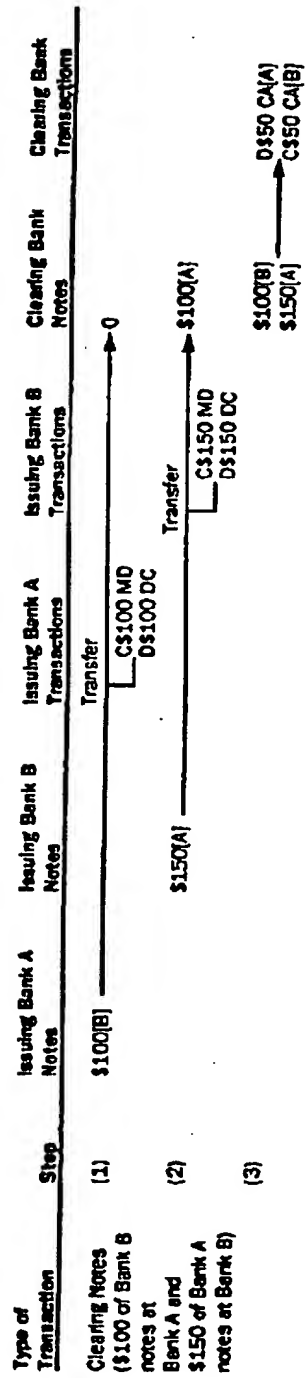
Key: () — Alternate values and steps

【図22】



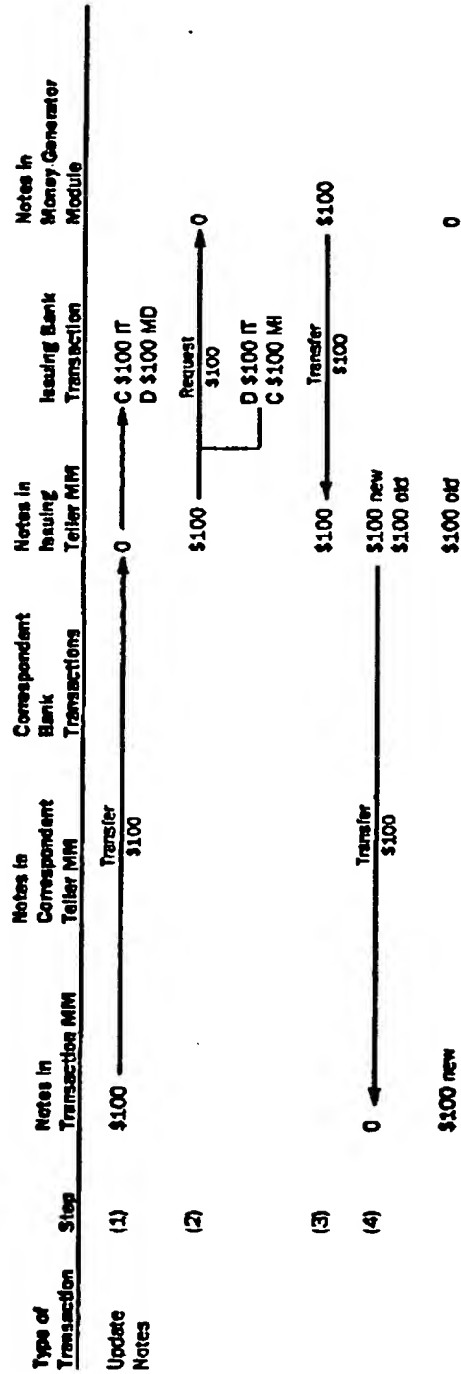
Key: () — Alternate values and steps

【図23】



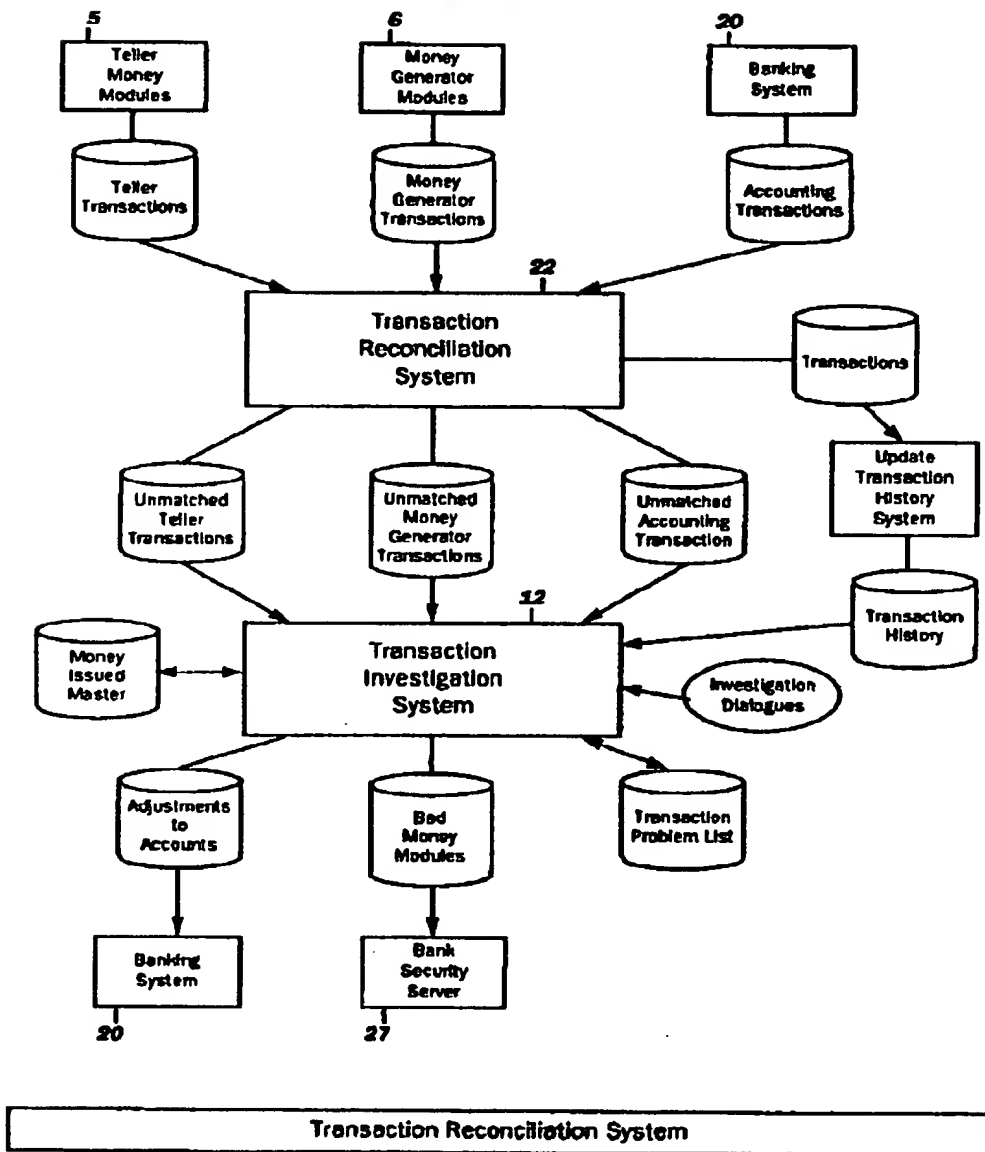
Key: () — Alternate values and steps

【図24】

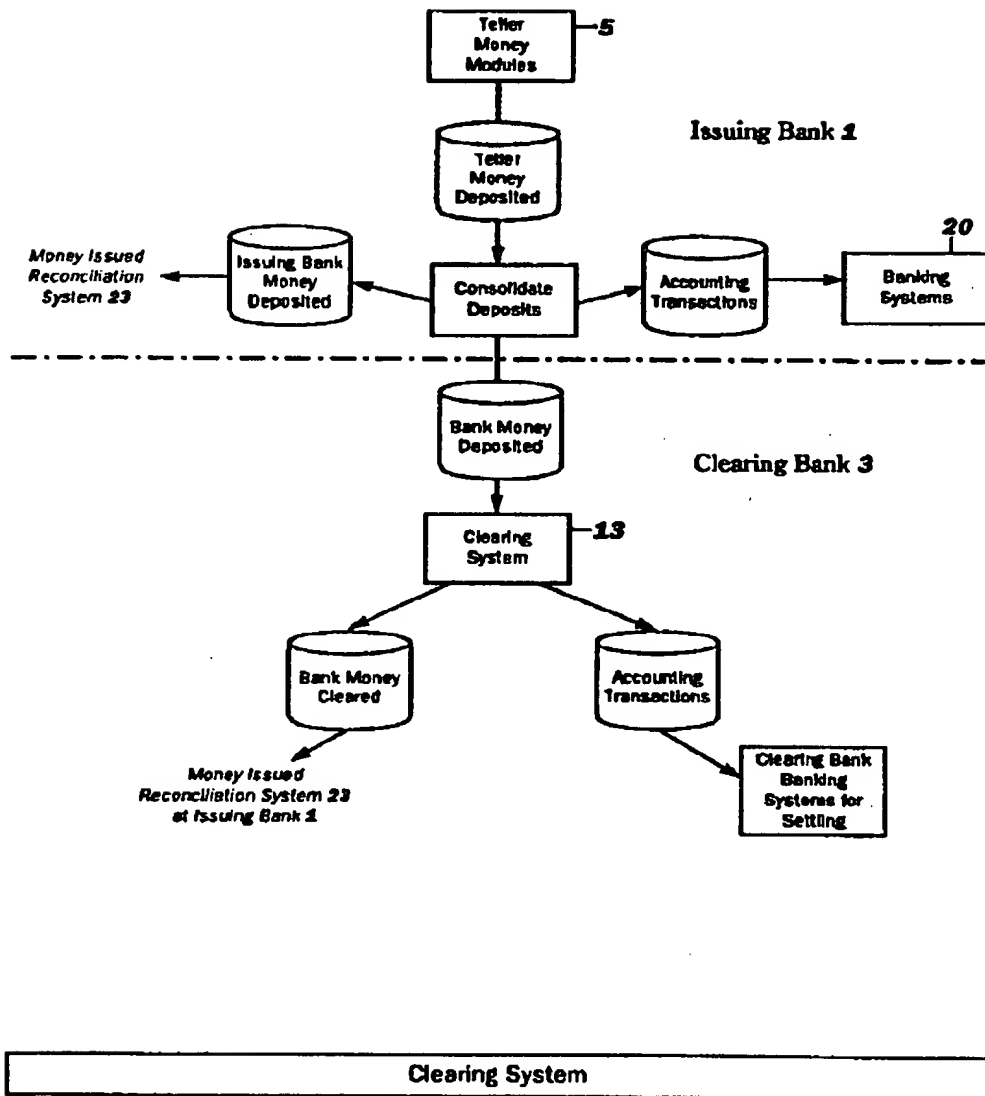


Key: () --- Alternate values and steps

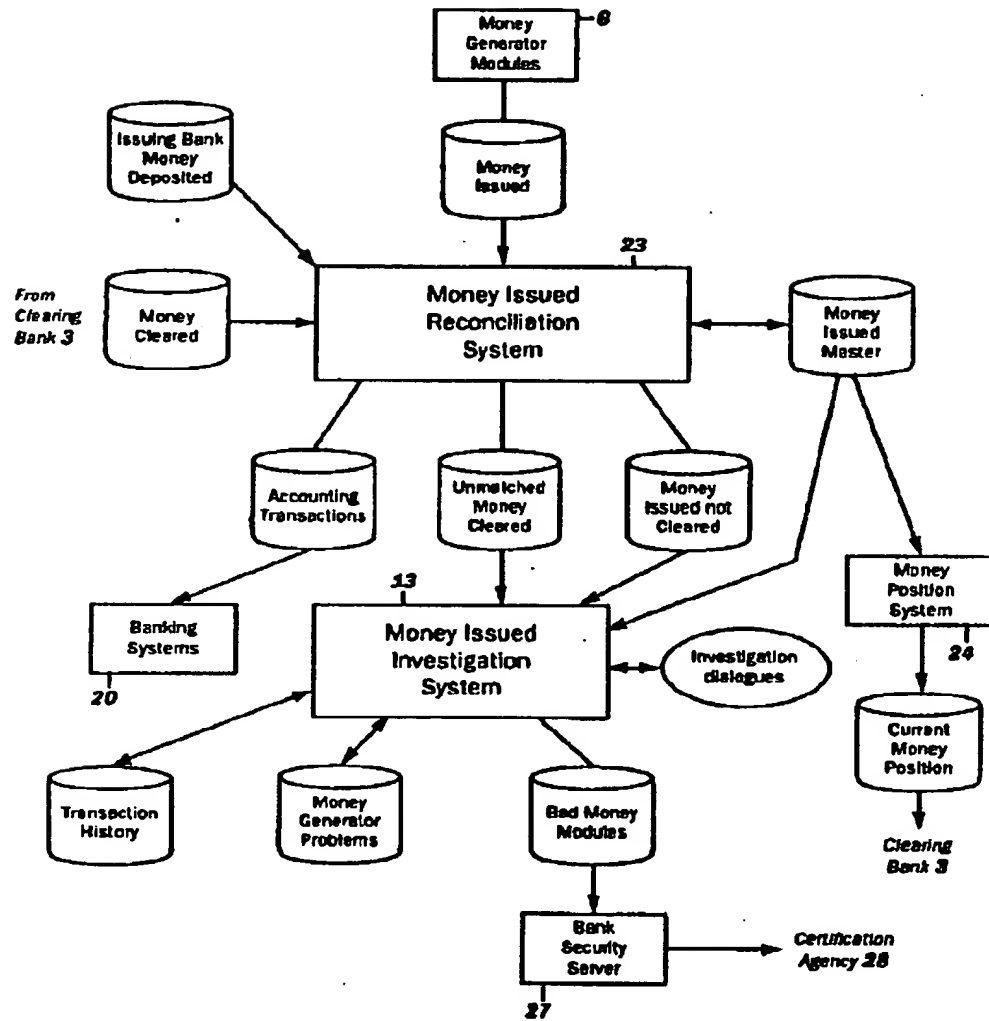
【図25】



【図26】

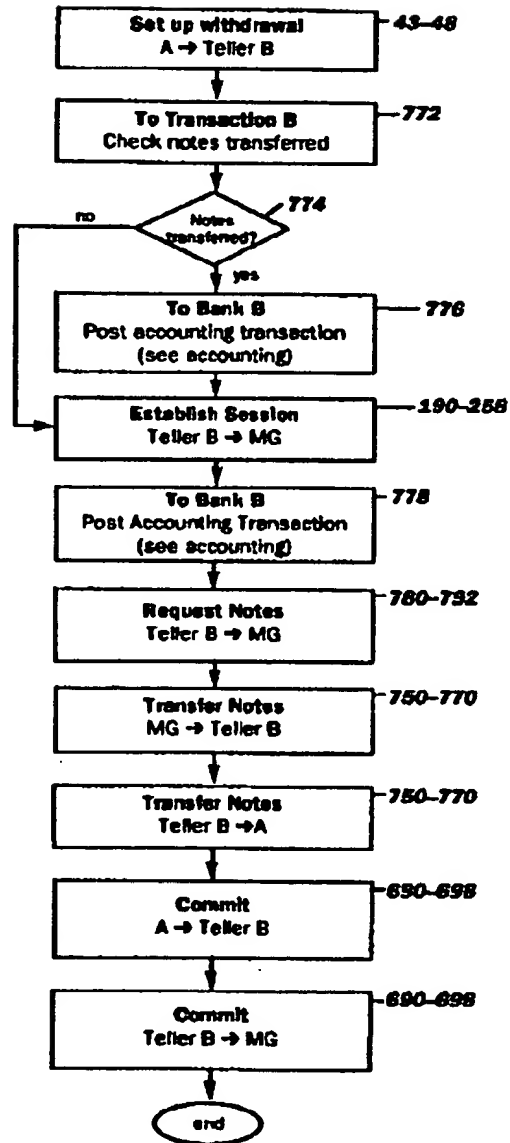


【図27】



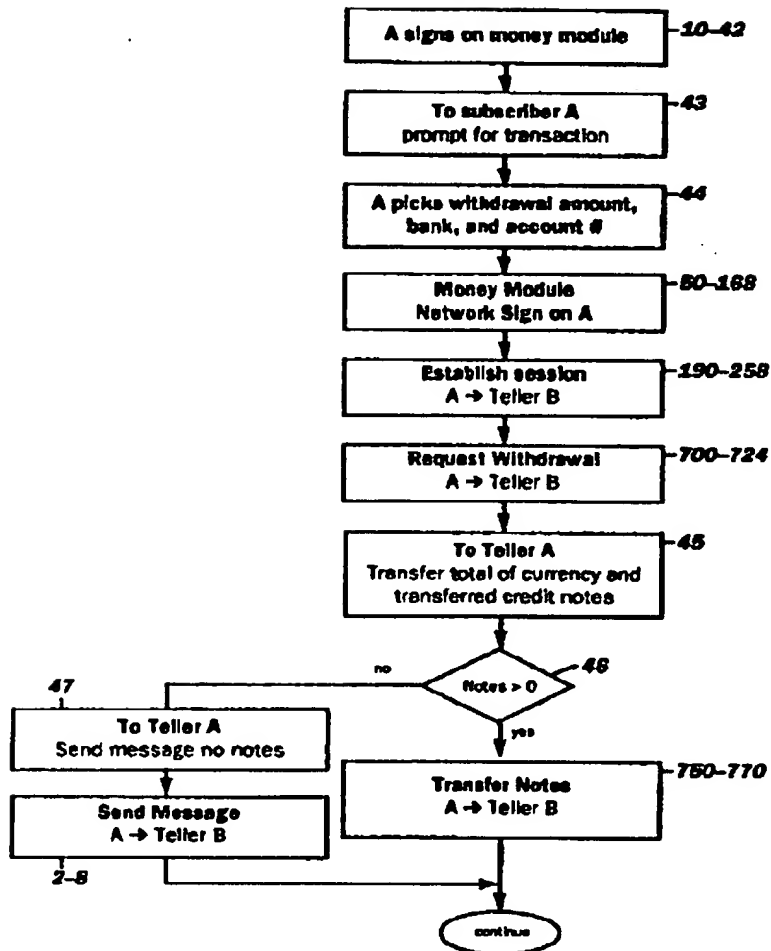
Money Issued Reconciliation System

【図28】



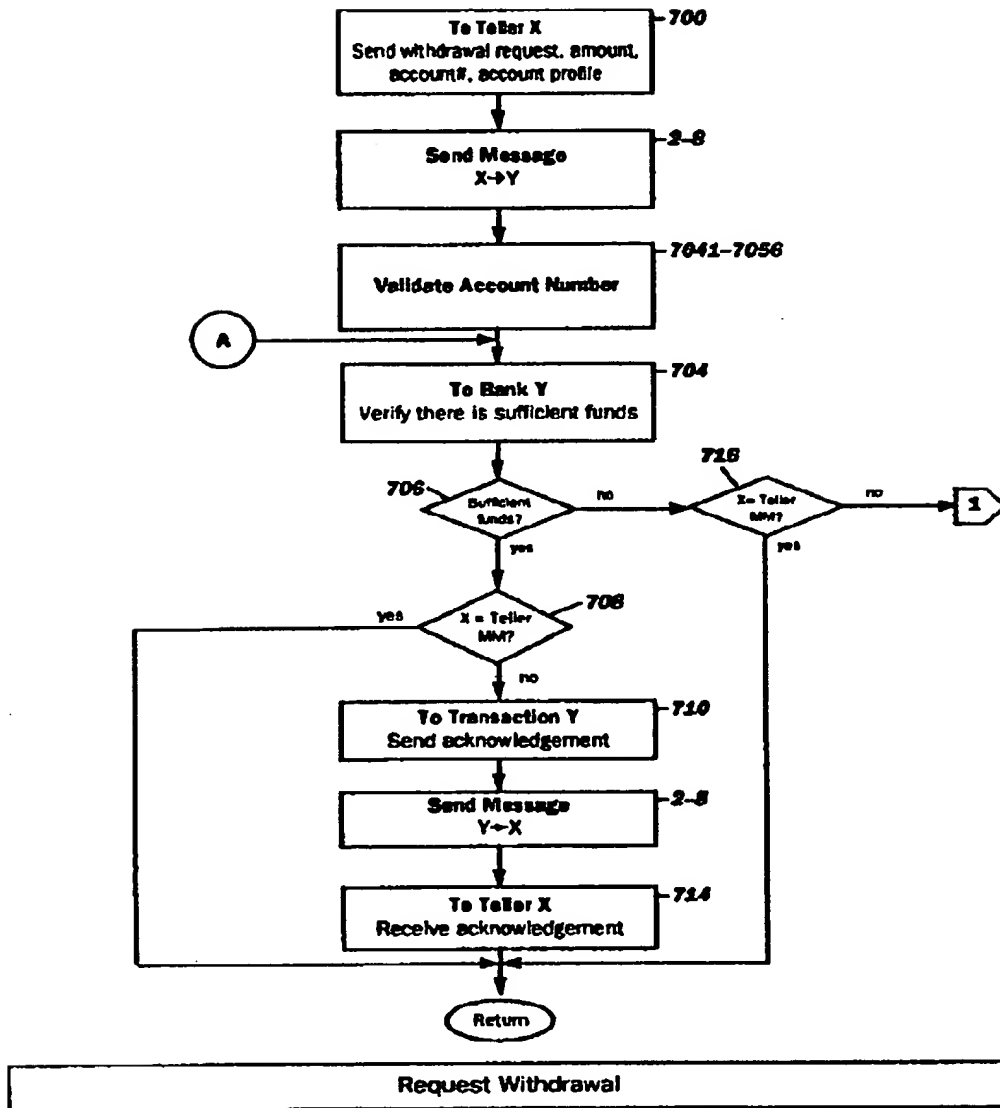
Withdrawal from Issuing Bank

【図29】

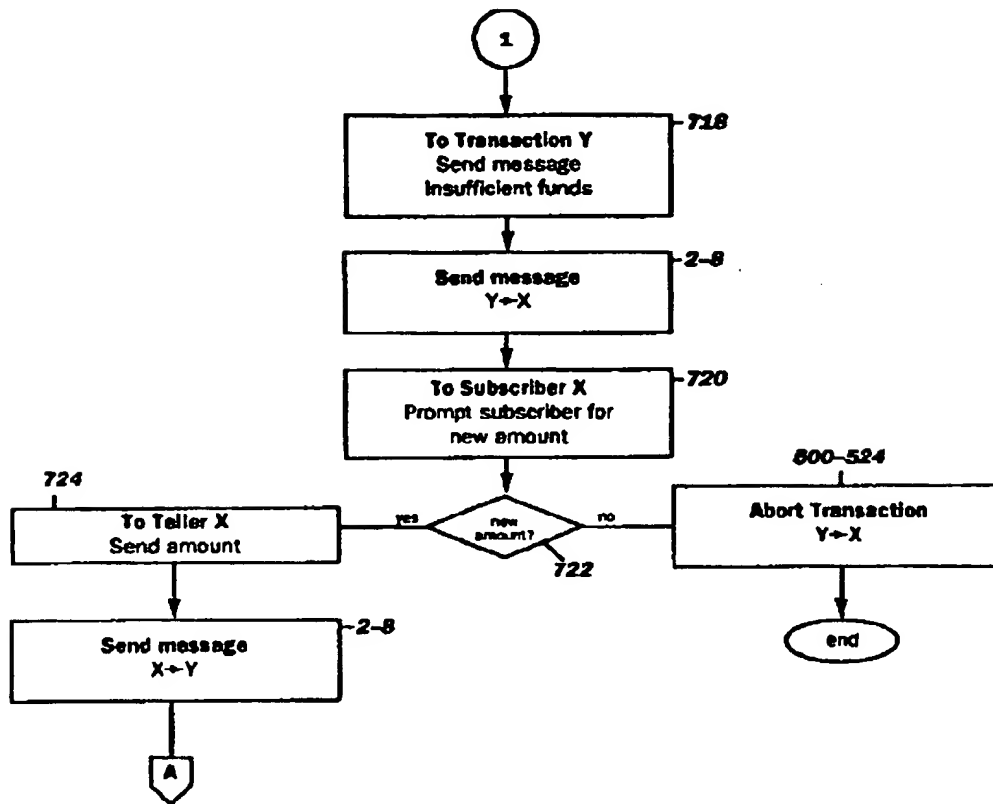


Setup Withdrawal

【図30】

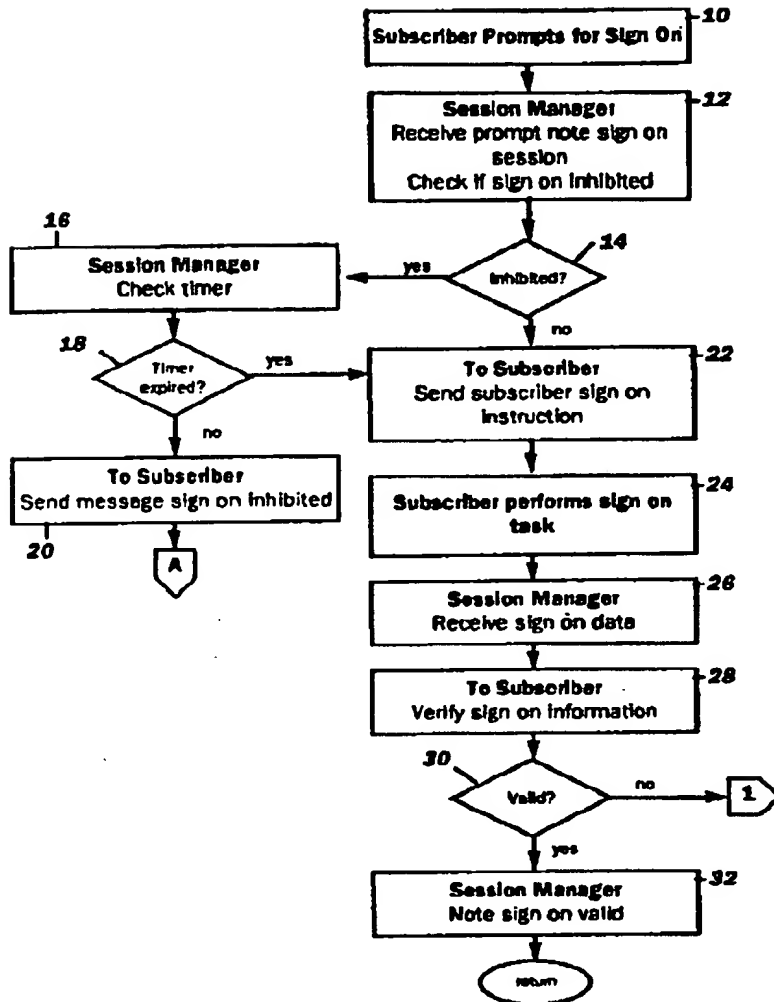


【図31】



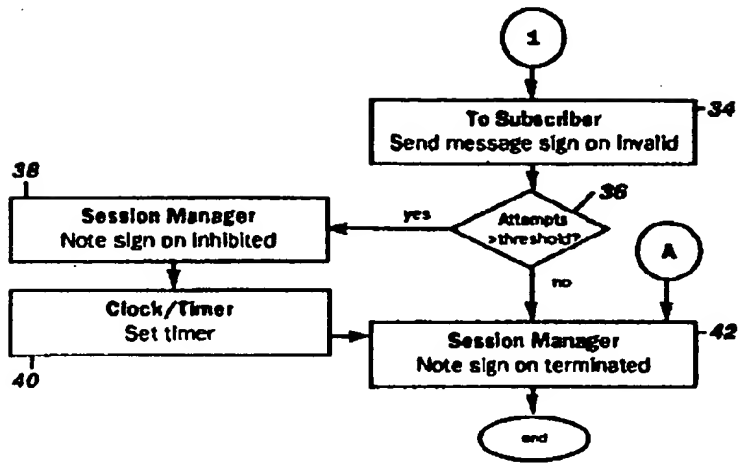
Request Withdrawal (continued)

【図32】



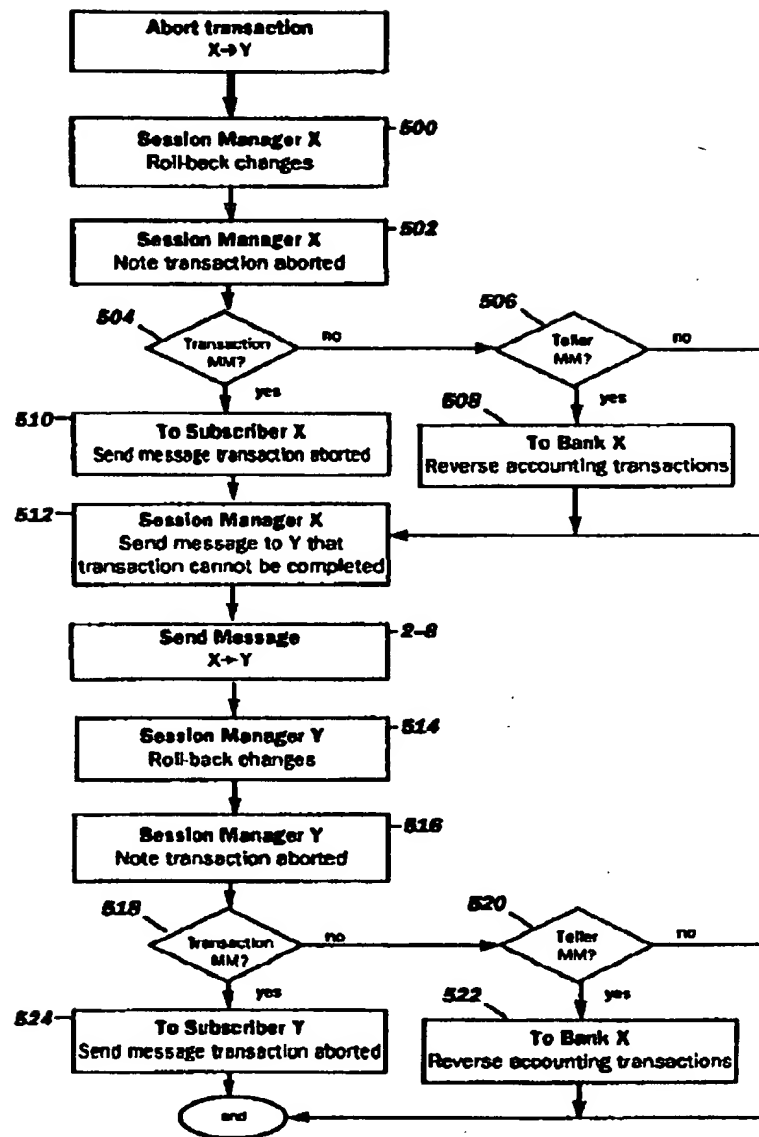
Subscriber Money Module Sign On

【図33】



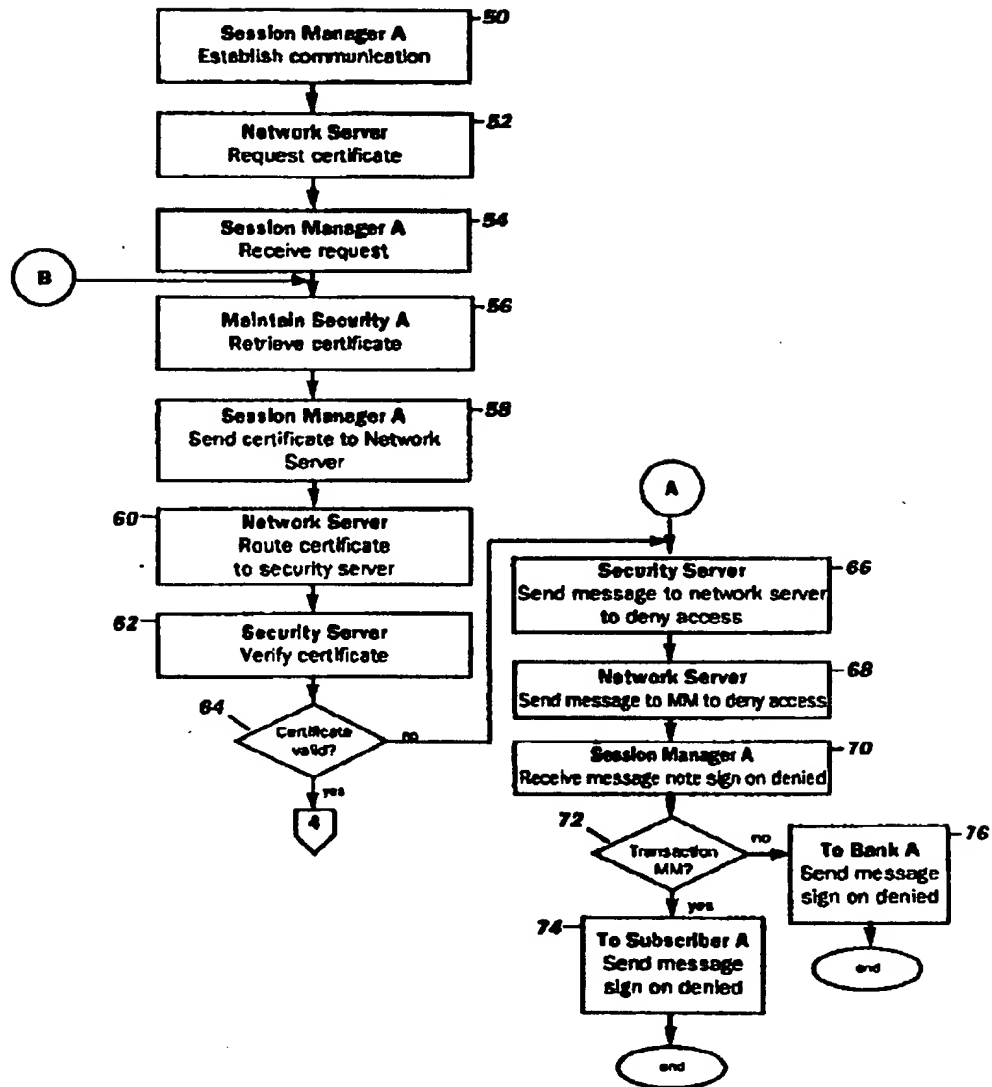
Subscriber Money Module Sign On

【図34】



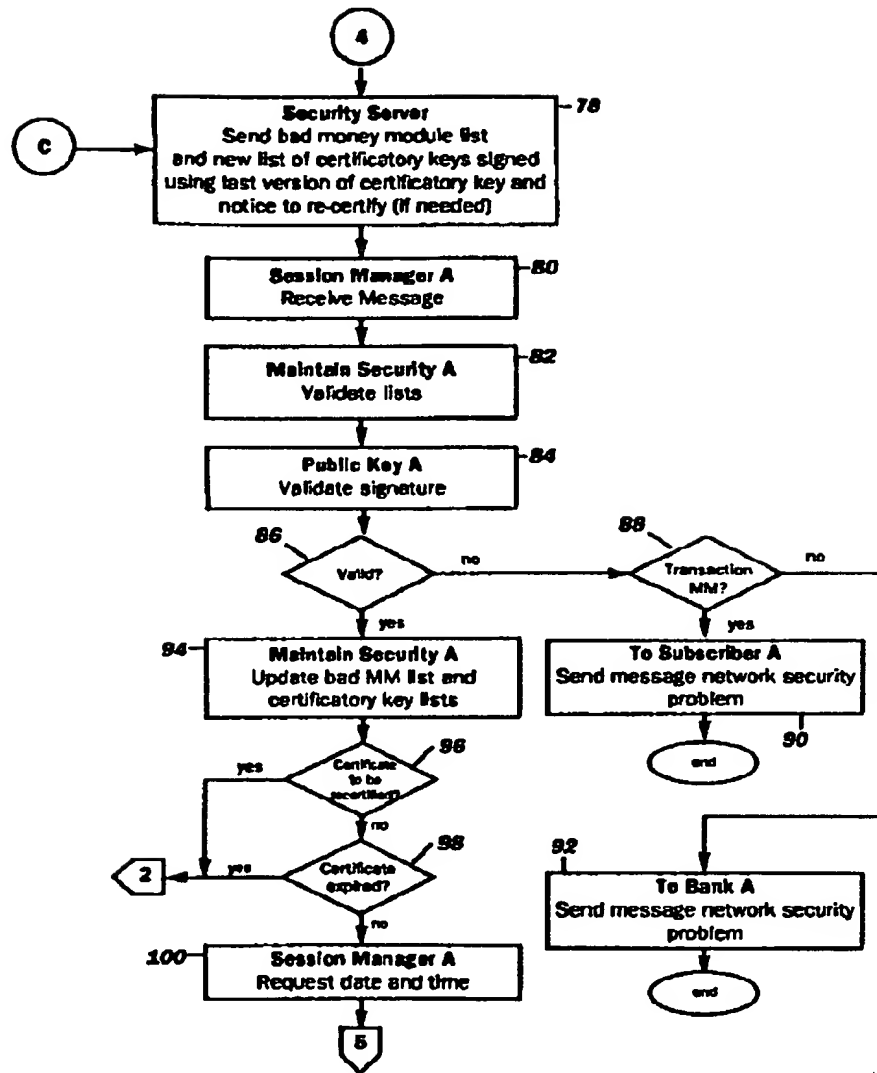
Abort Transaction Money Module to Money Module

【図35】



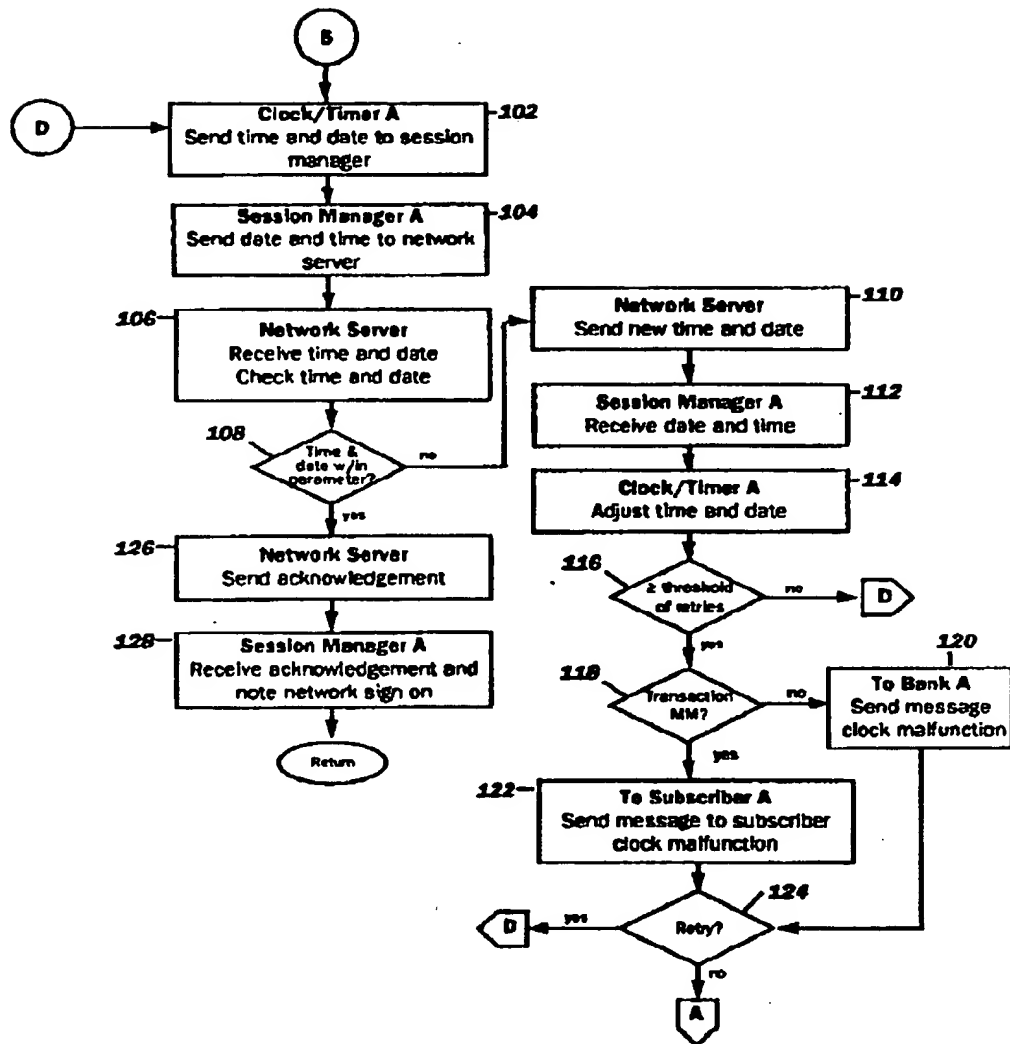
Money Module Network Sign On

【図36】



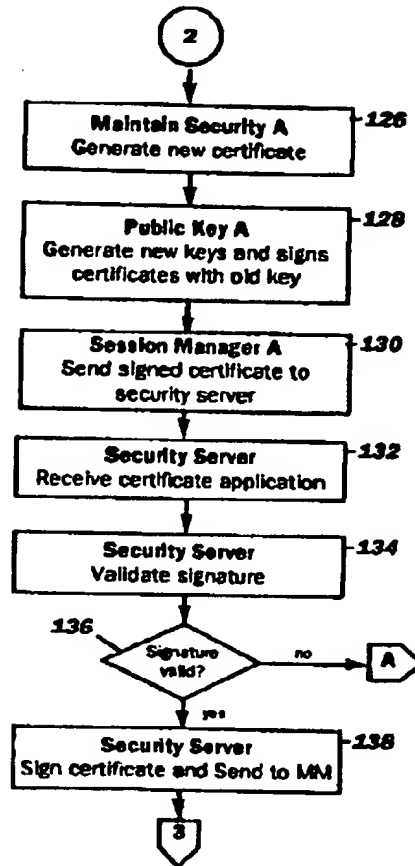
Money Module Network Sign On (continued)

【図37】



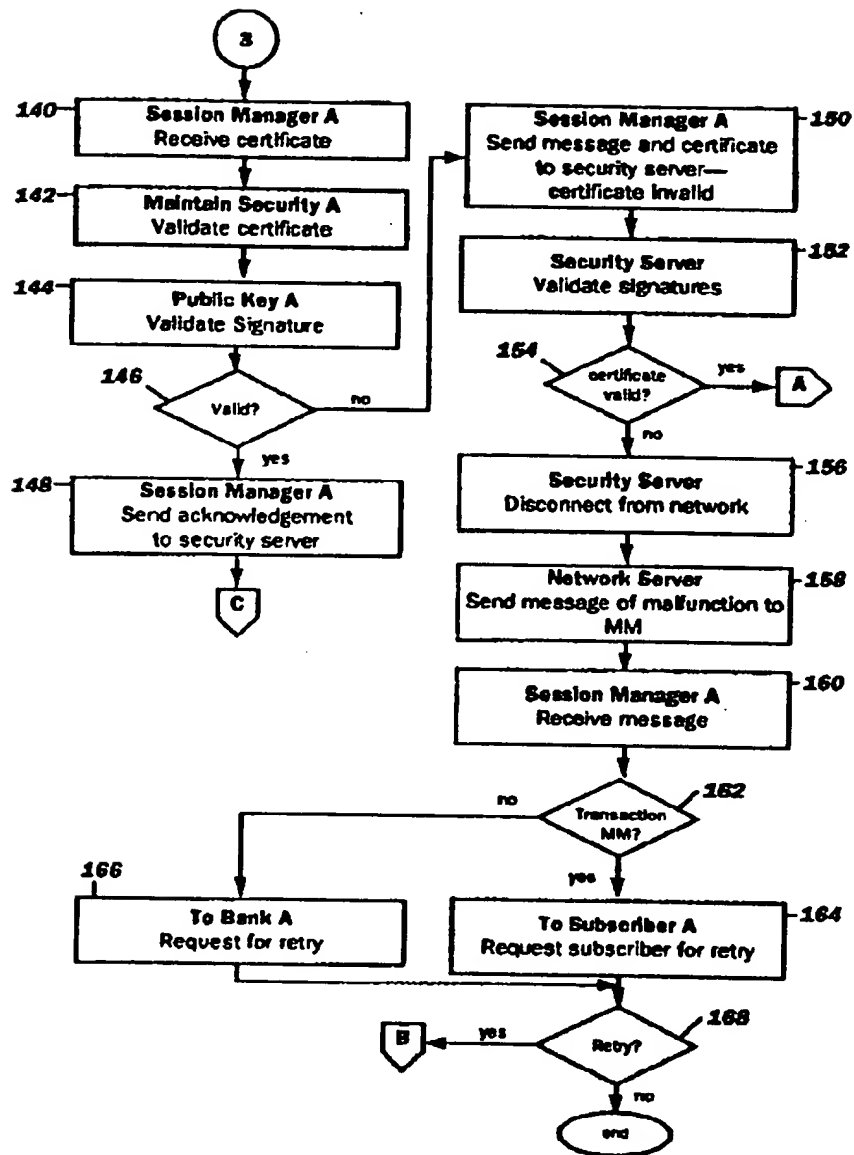
Money Module Network Sign On (continued)

【図38】



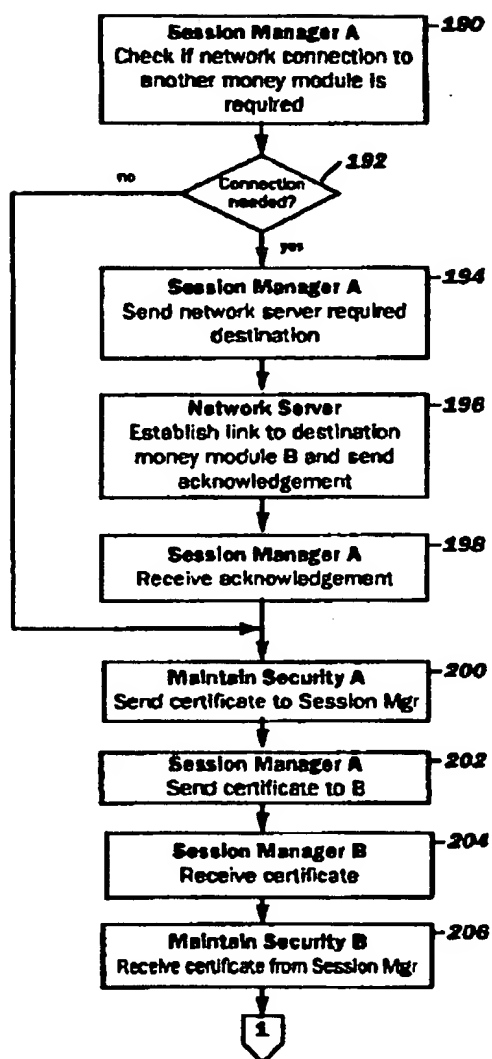
Money Module Network Sign On (continued)

【図39】



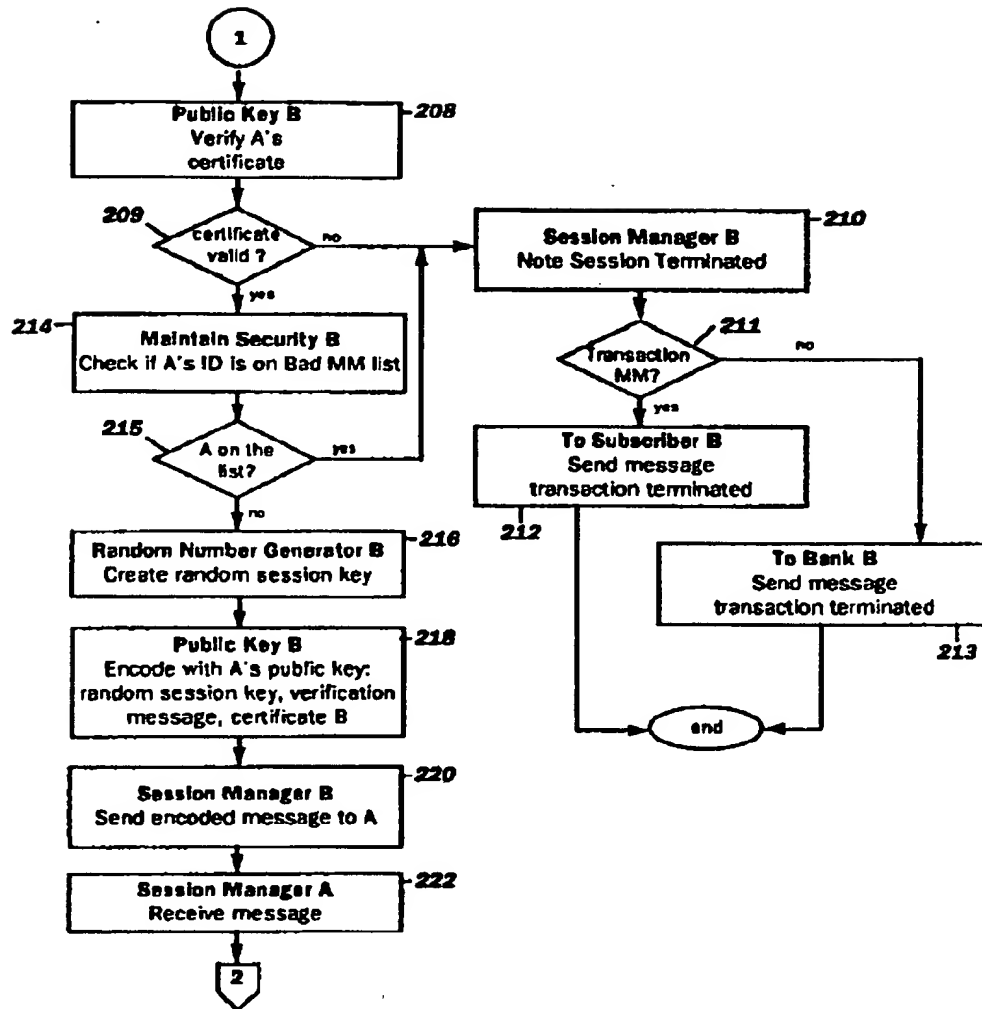
Money Module Network Sign On (continued)

【図40】



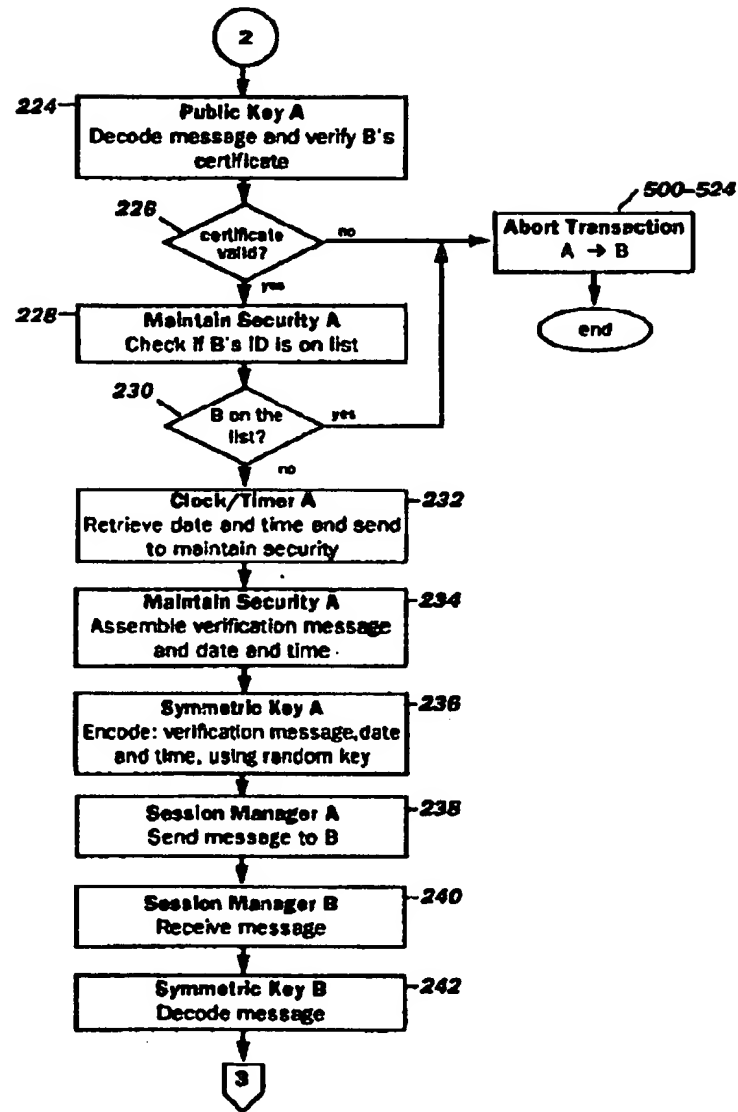
Establish Session — Money Module to Money Module

【図41】



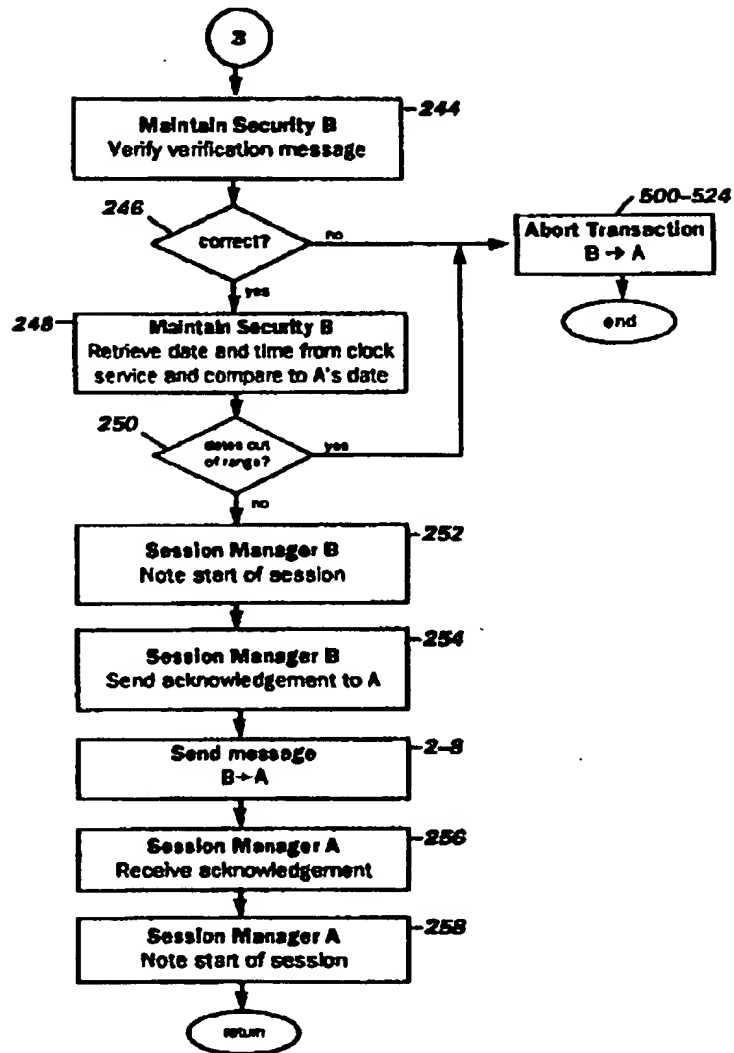
Establish Session — Money Module to Money Module (continued)

【図42】



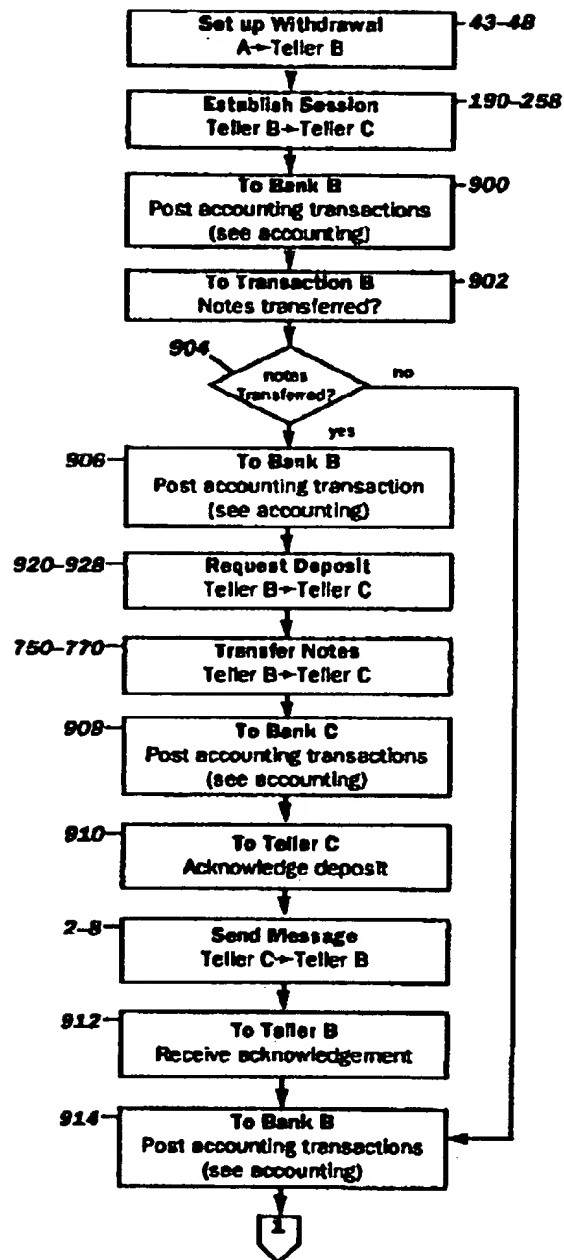
Establish Session — Money Module to Money Module (continued)

【図43】



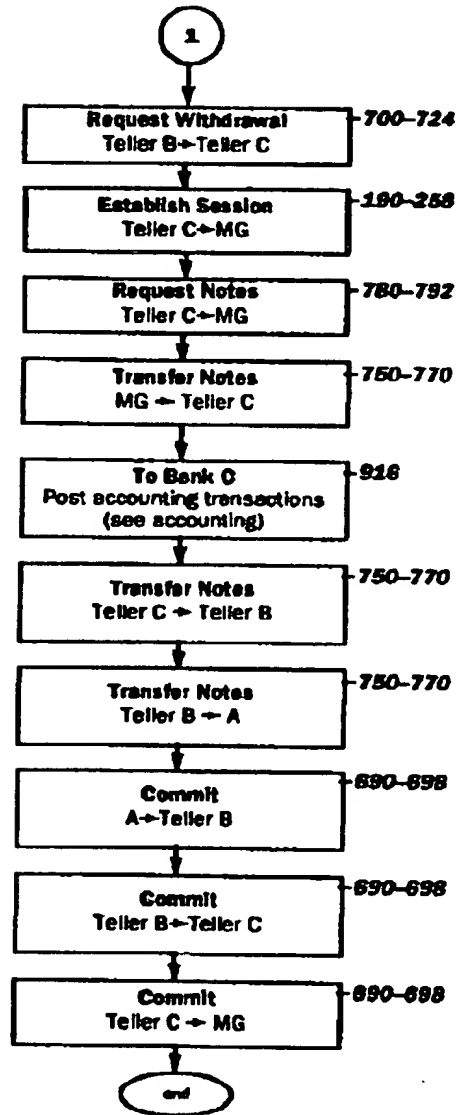
Establish Session — Money Module to Money Module (continued)

【図44】



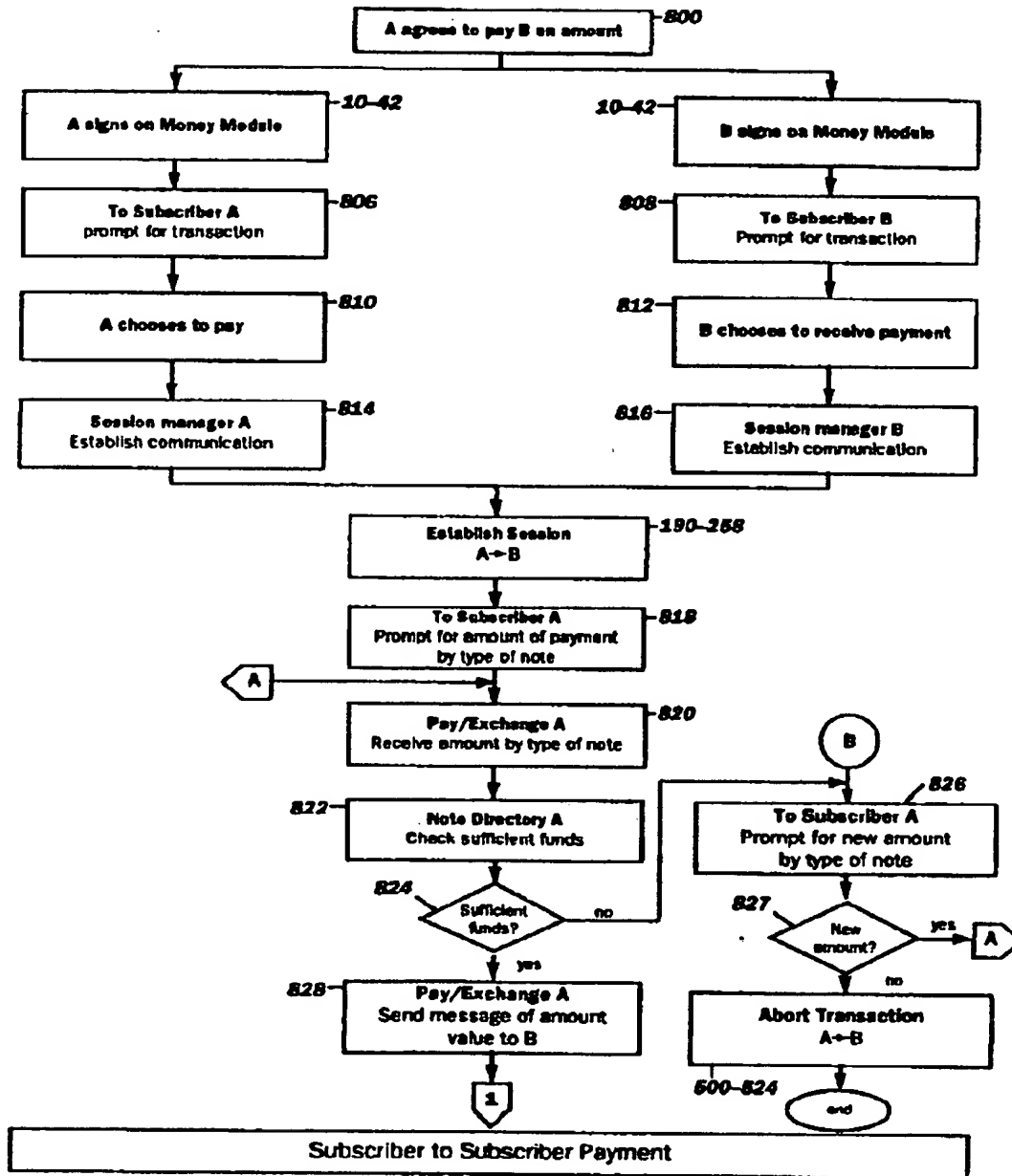
Withdrawal from Correspondent Bank

【図45】

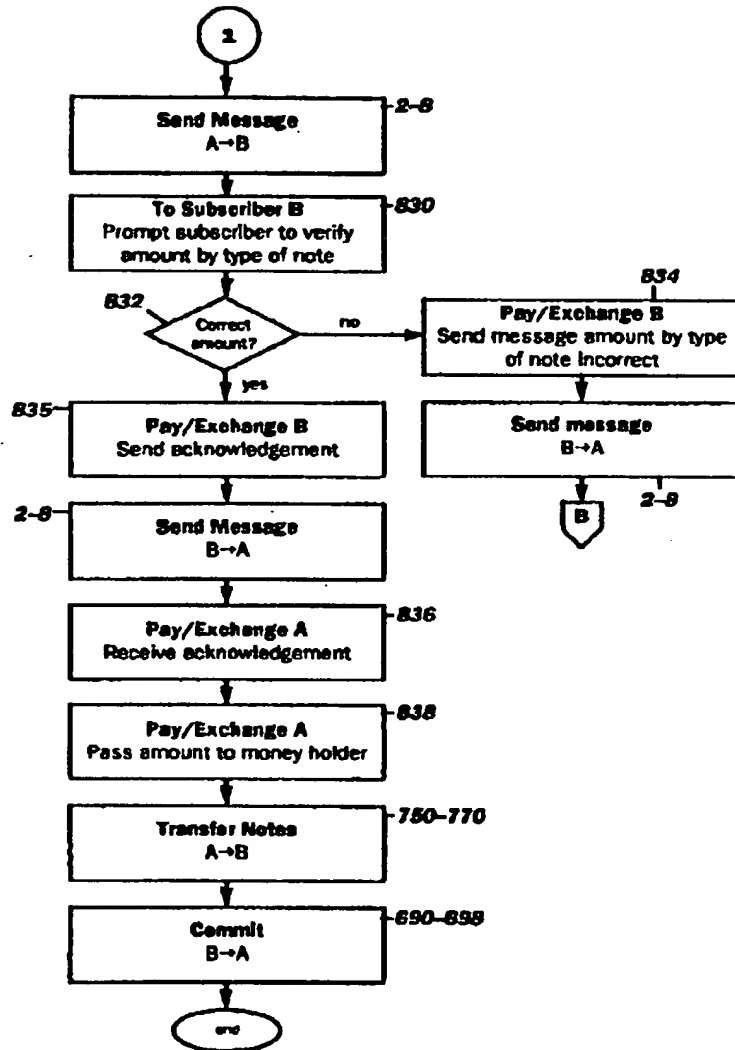


Withdrawal from Correspondent Bank (continued)

【図46】

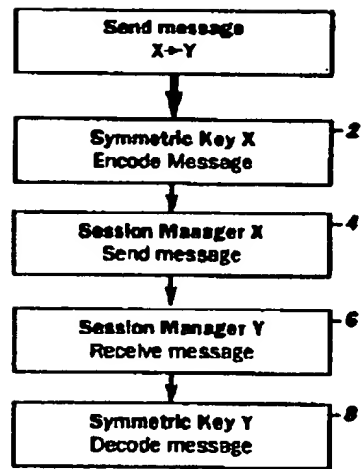


【図47】



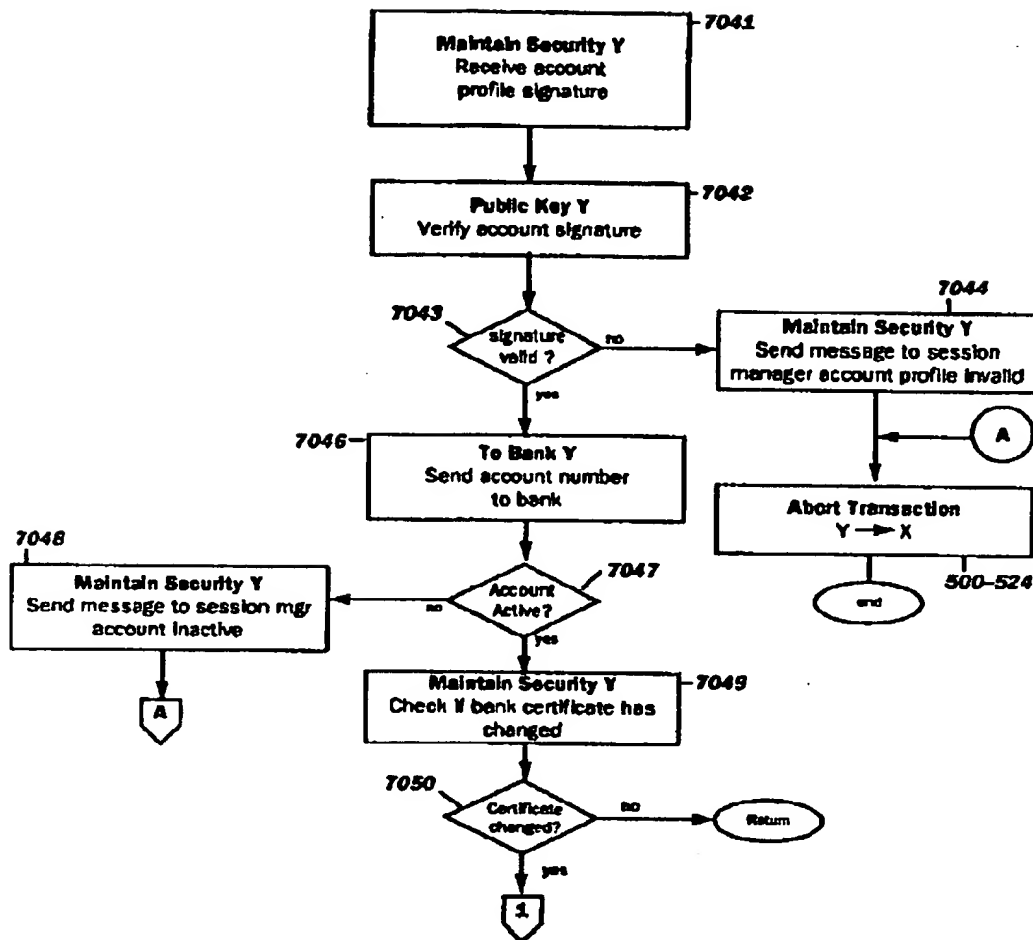
Subscriber to Subscriber Payment (continued)

【図48】



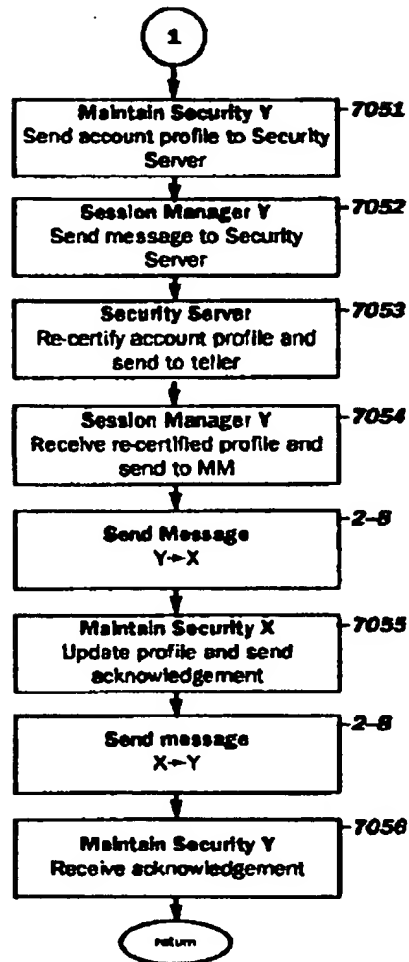
Send Encoded Message — Money Module to Money Module

【図49】



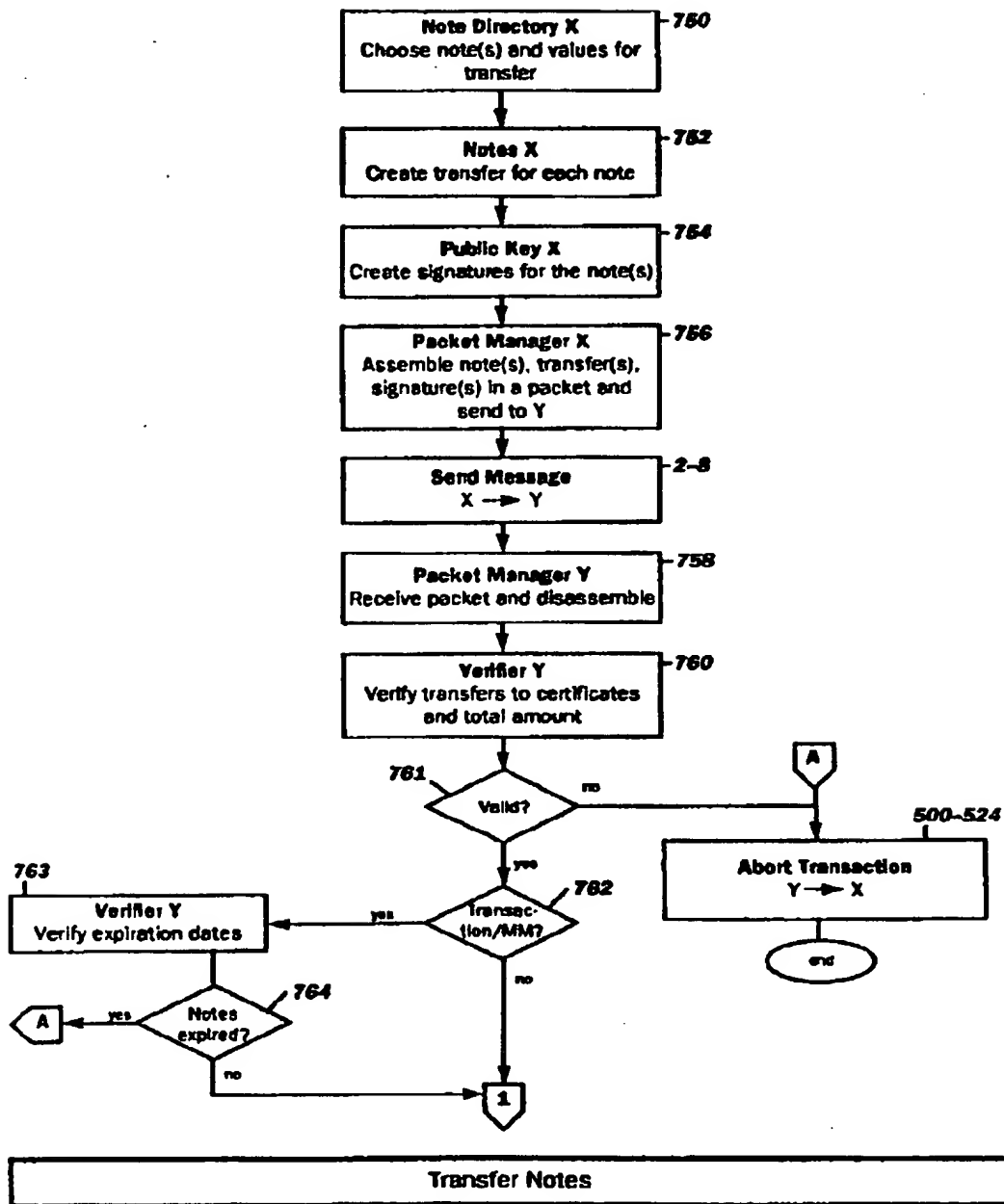
Validate Account Number

【図50】

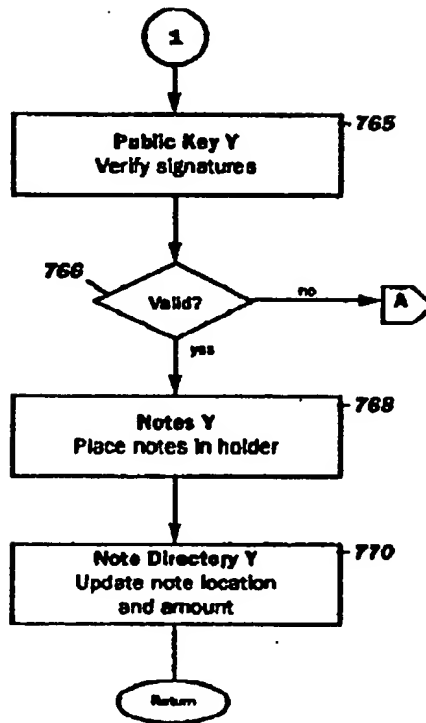


Validate Account Number (continued)

【図51】

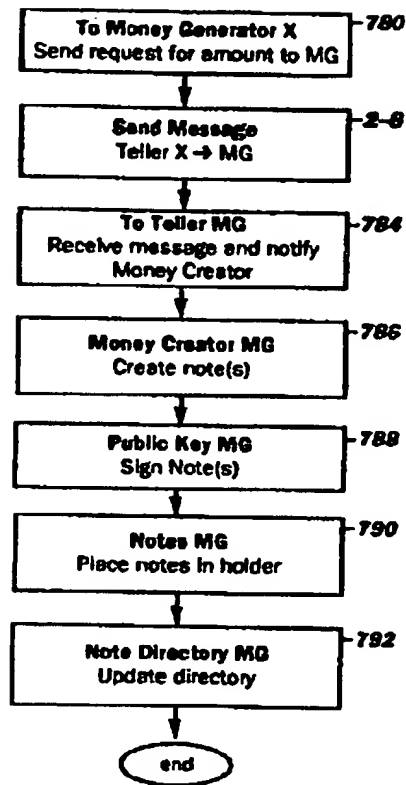


【図52】



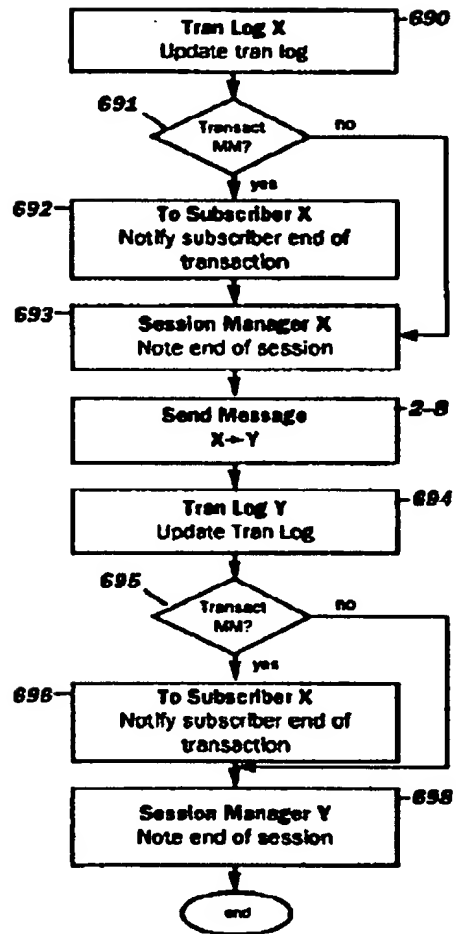
Transfer Notes (continued)

【図53】



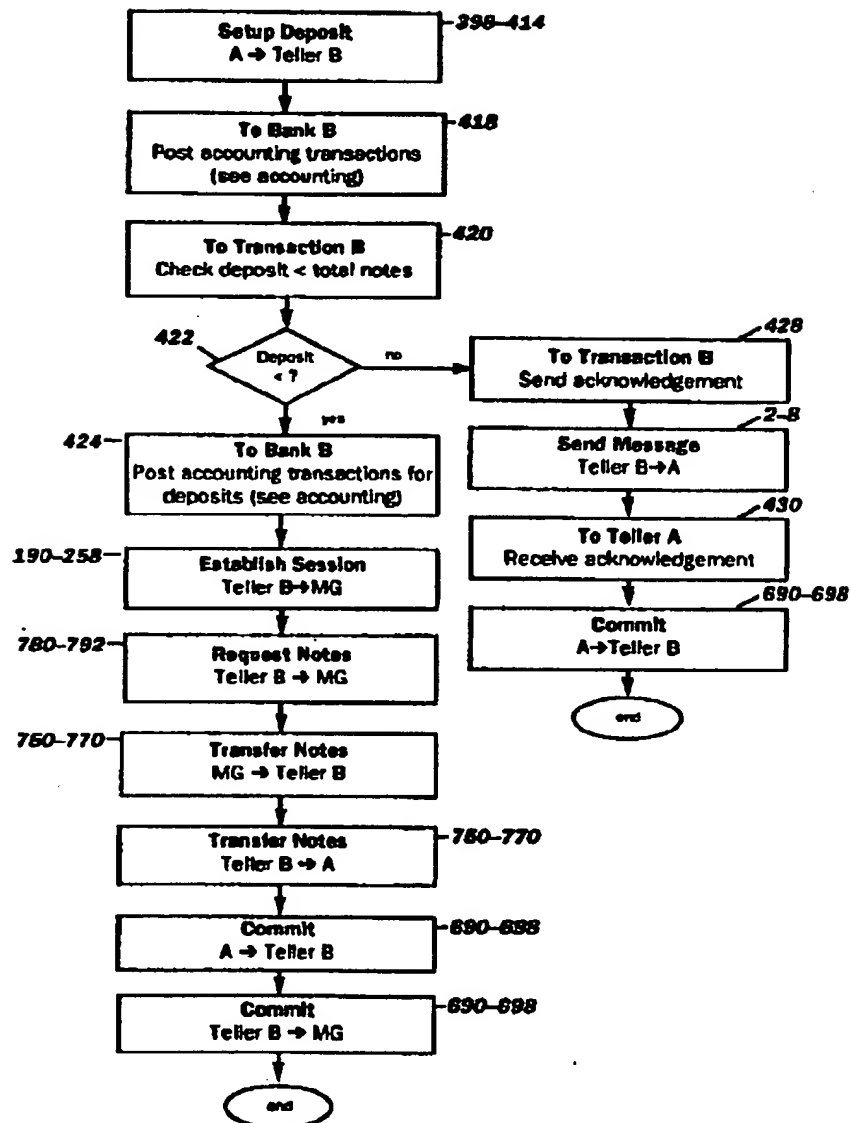
Request Notes

【図54】



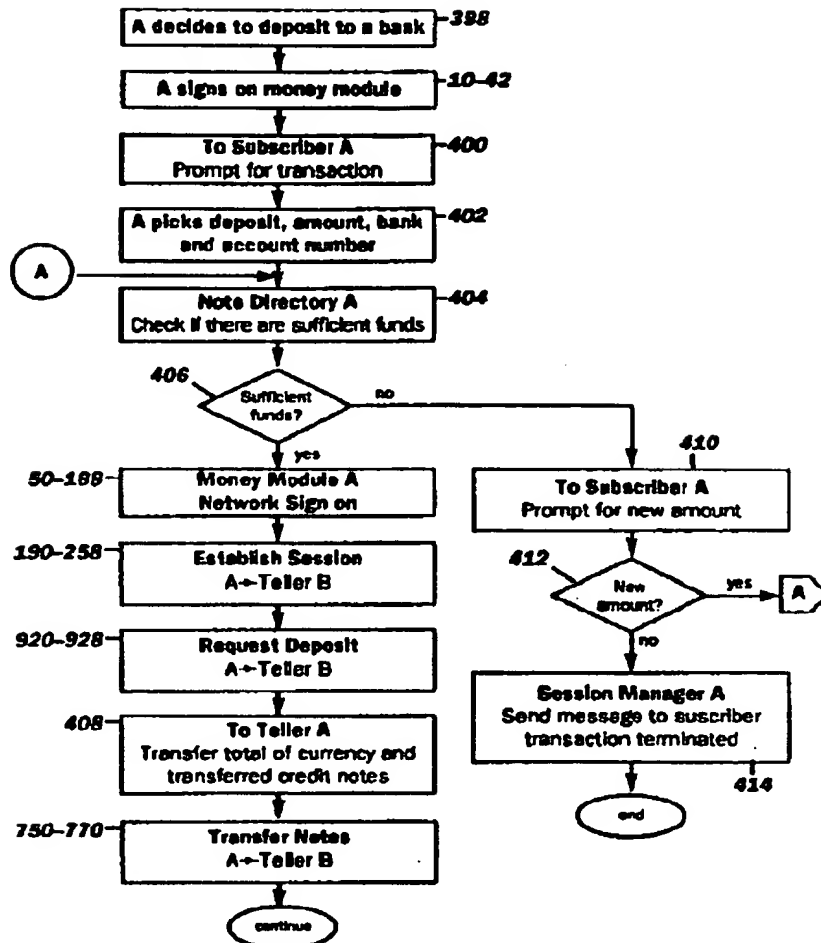
Commit

【図55】



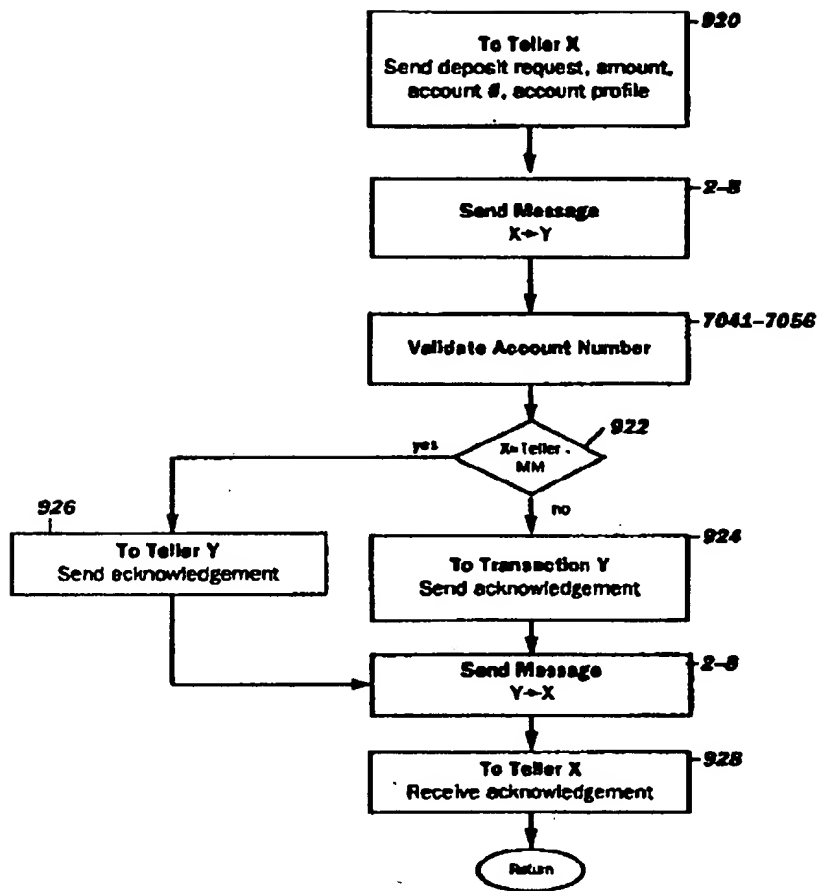
Deposit to Issuing Bank

【図56】



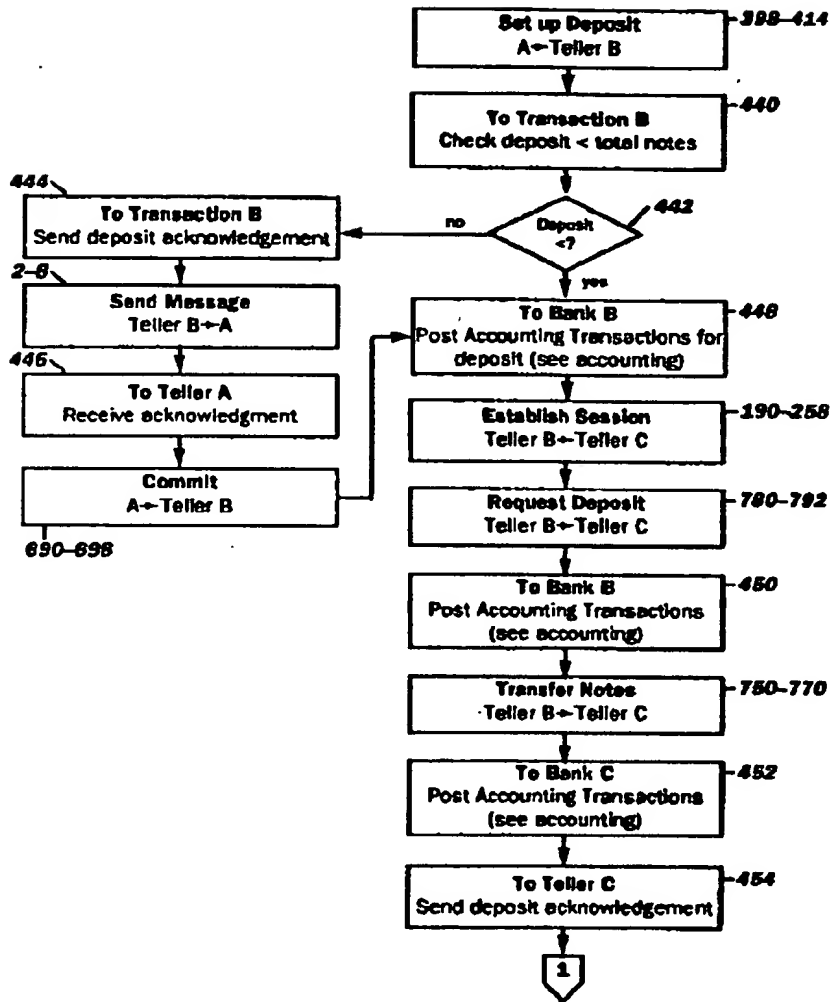
Set Up Deposit

【図57】



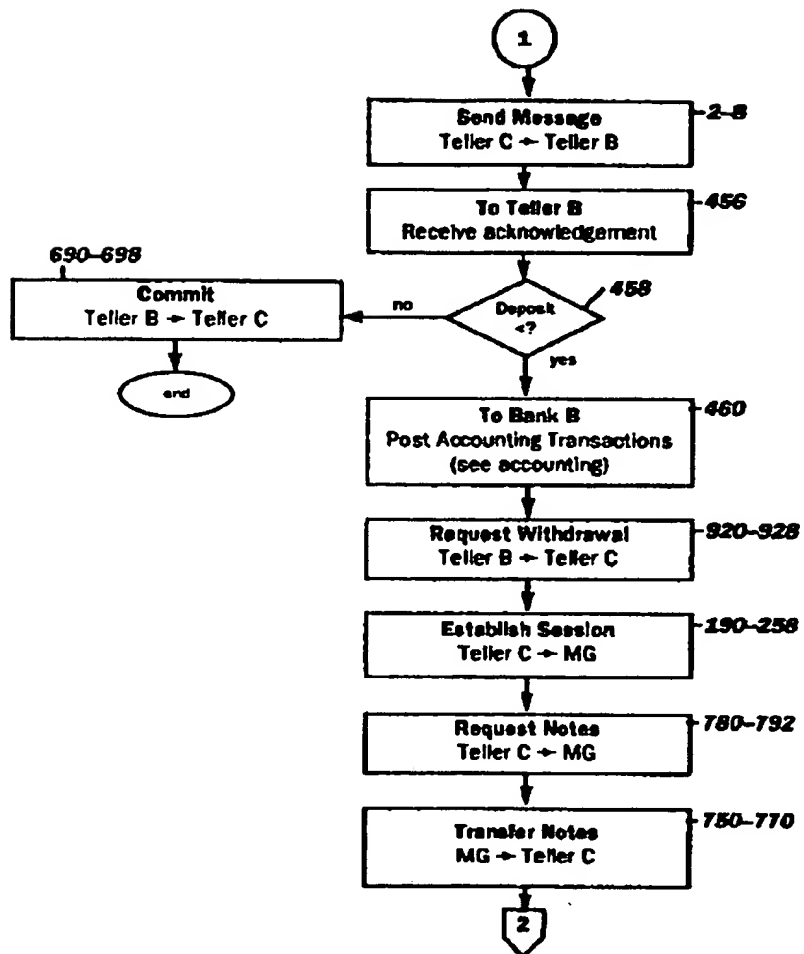
Request Deposit

【図58】



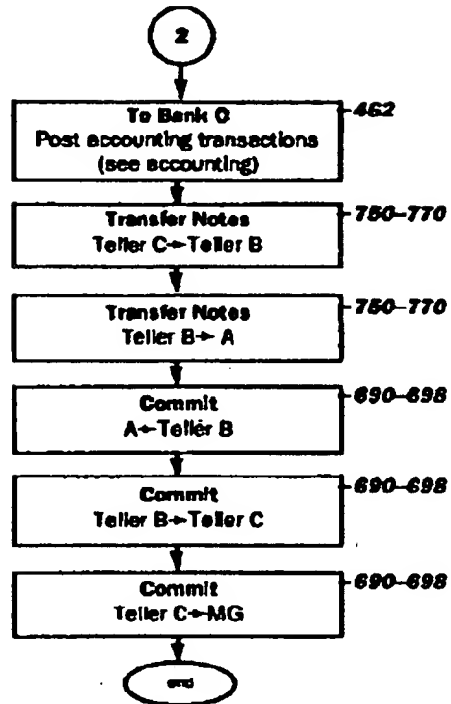
Deposit to Correspondent Bank

【図59】



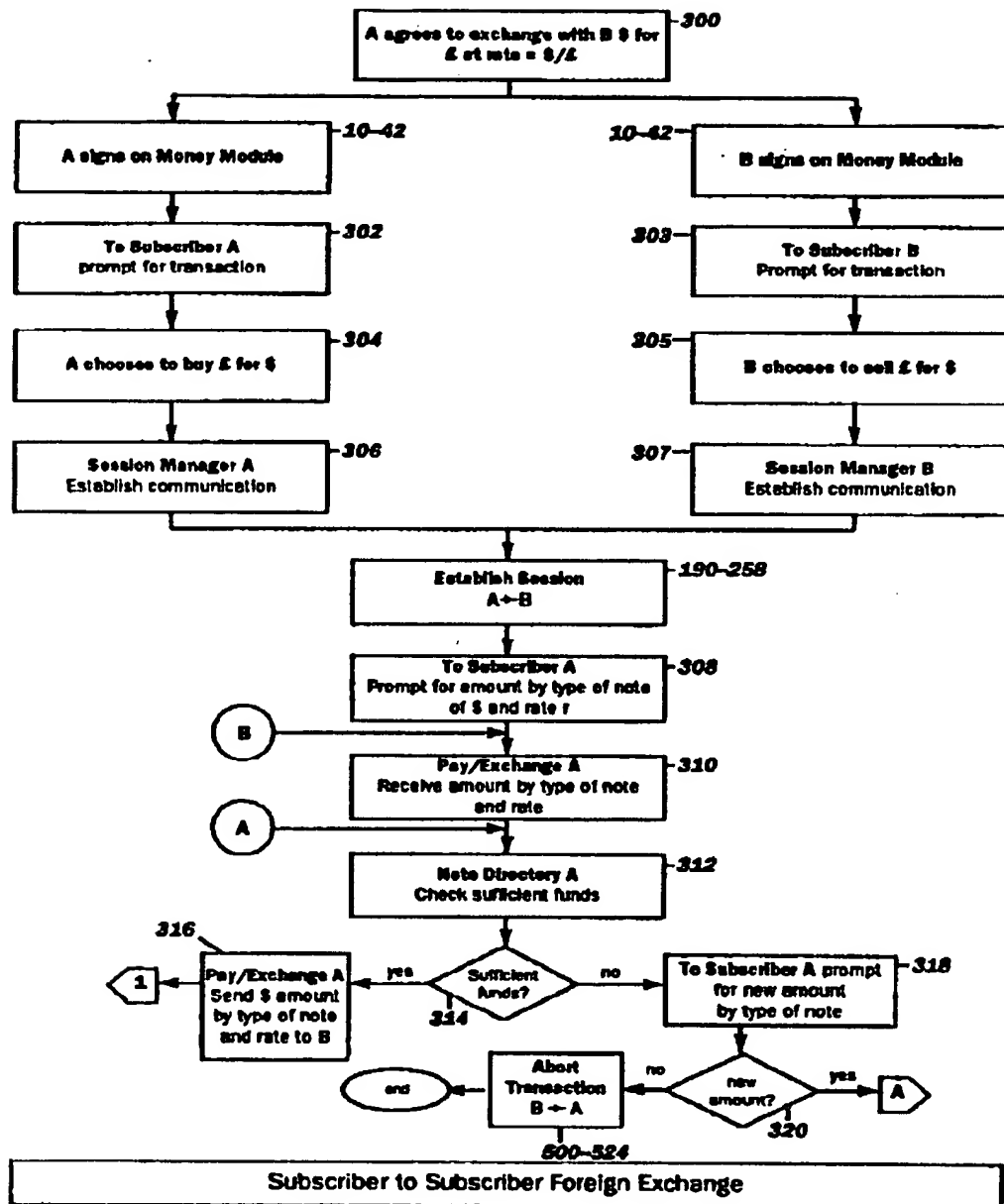
Deposit to Correspondent Bank (continued)

【図60】

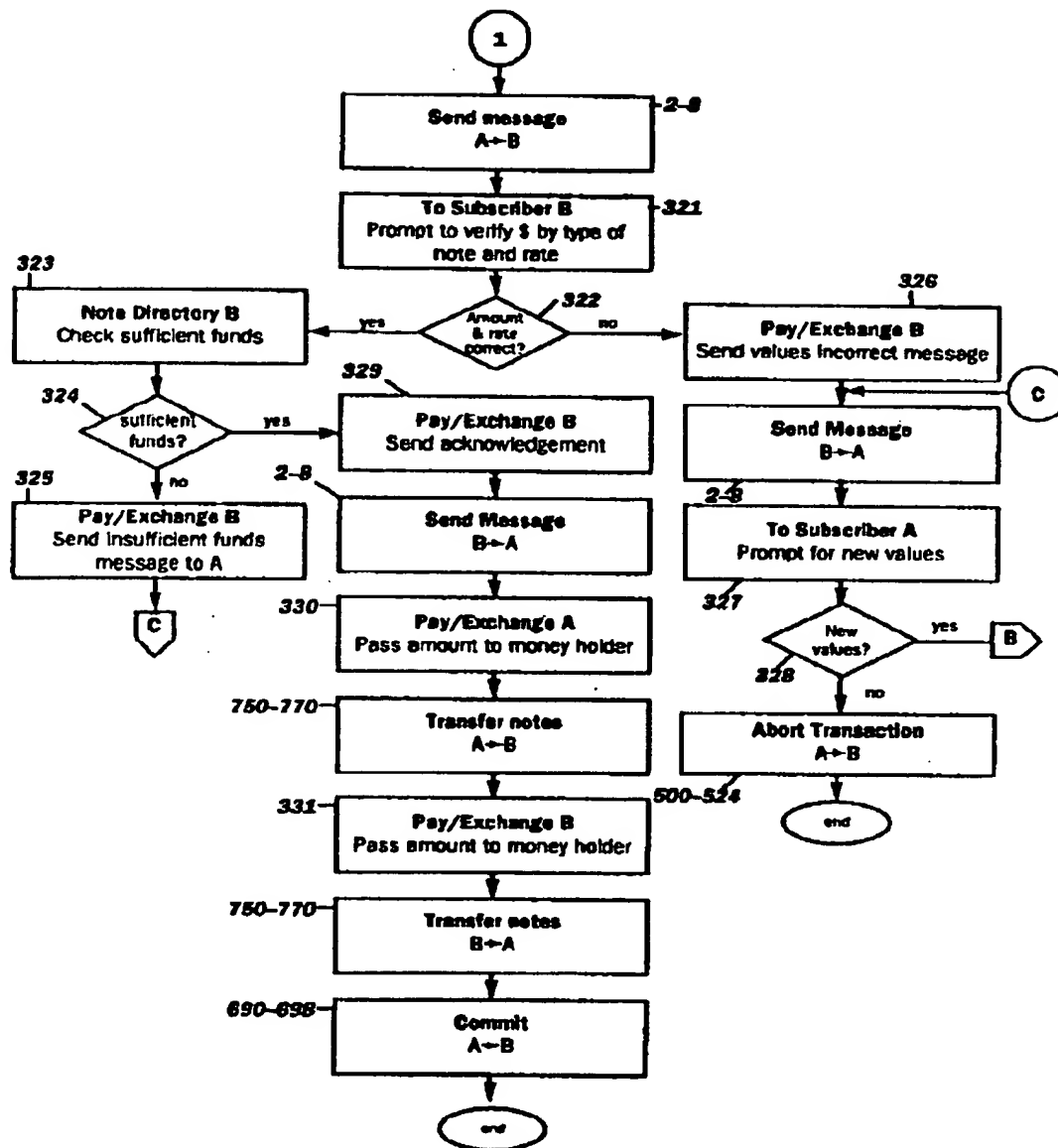


Deposit to Correspondent Bank (continued)

【図61】

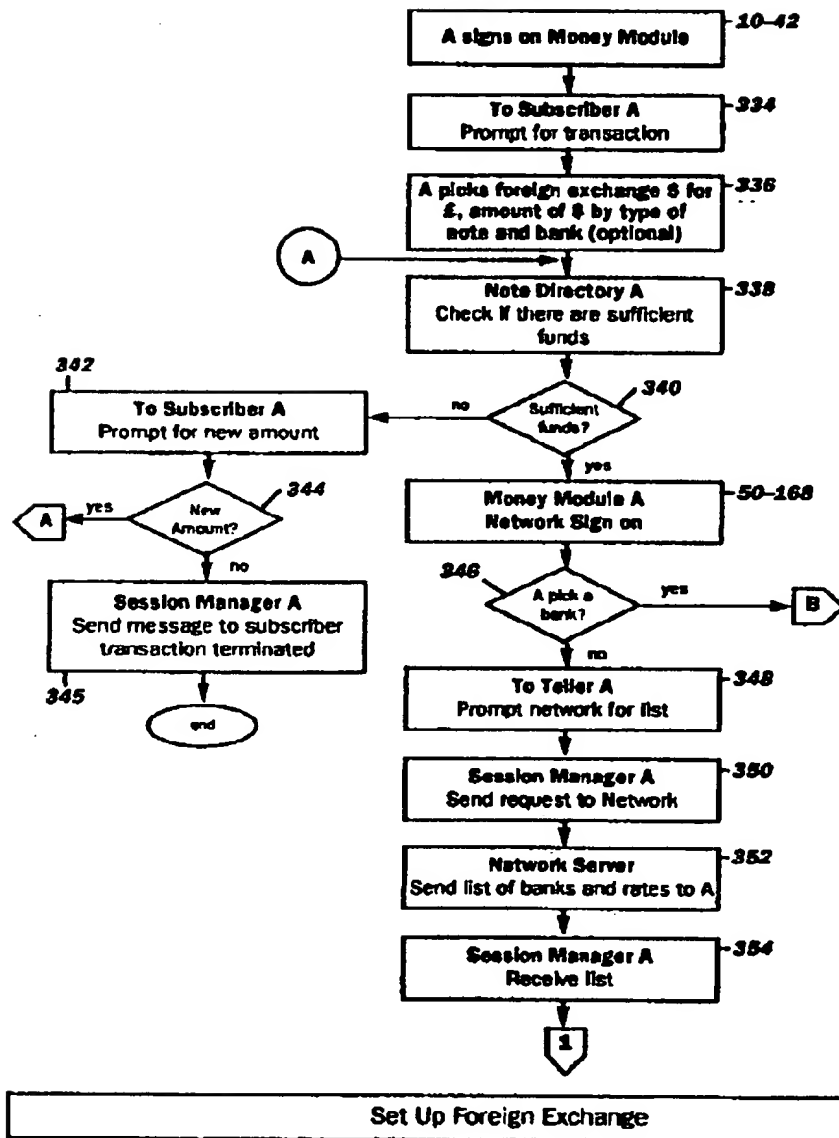


【図62】

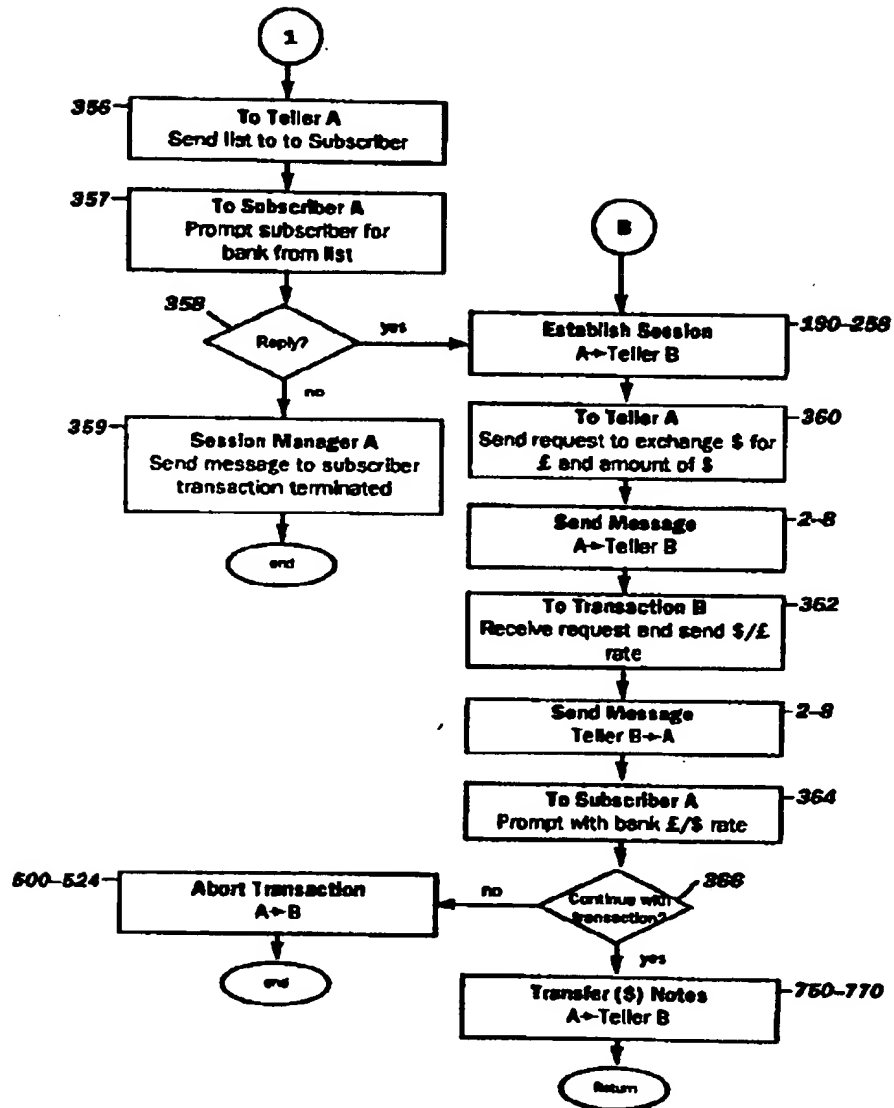


Subscriber to Subscriber Foreign Exchange (continued)

【図63】

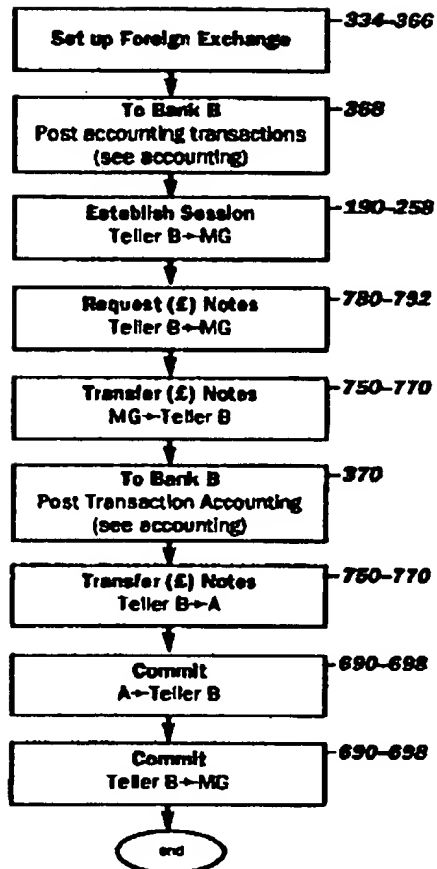


【図64】



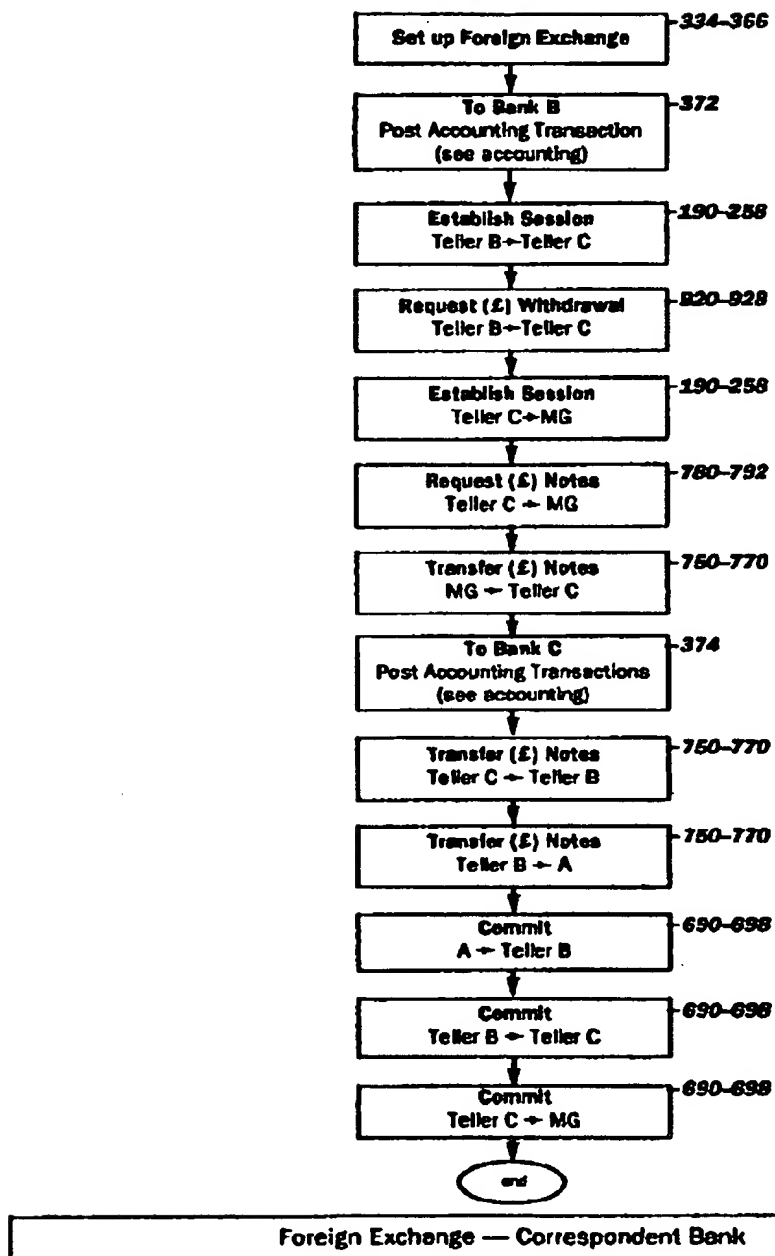
Set Up Foreign Exchange (continued)

【図65】

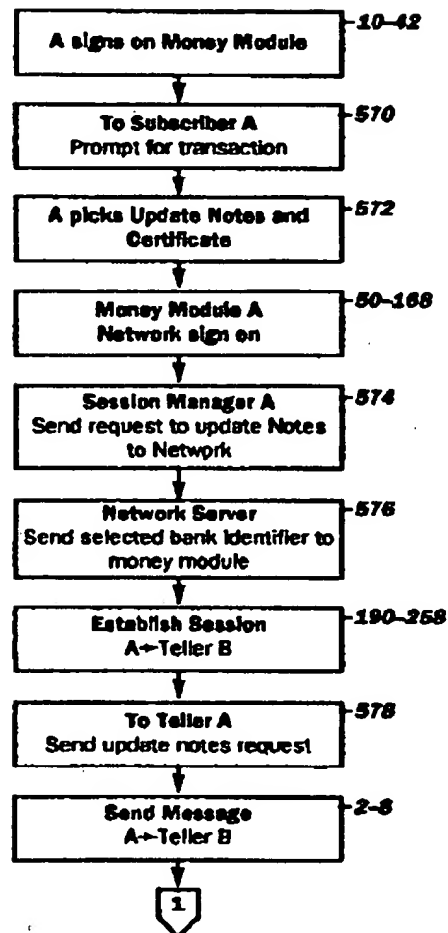


Foreign Exchange — Issuing Bank

【図66】

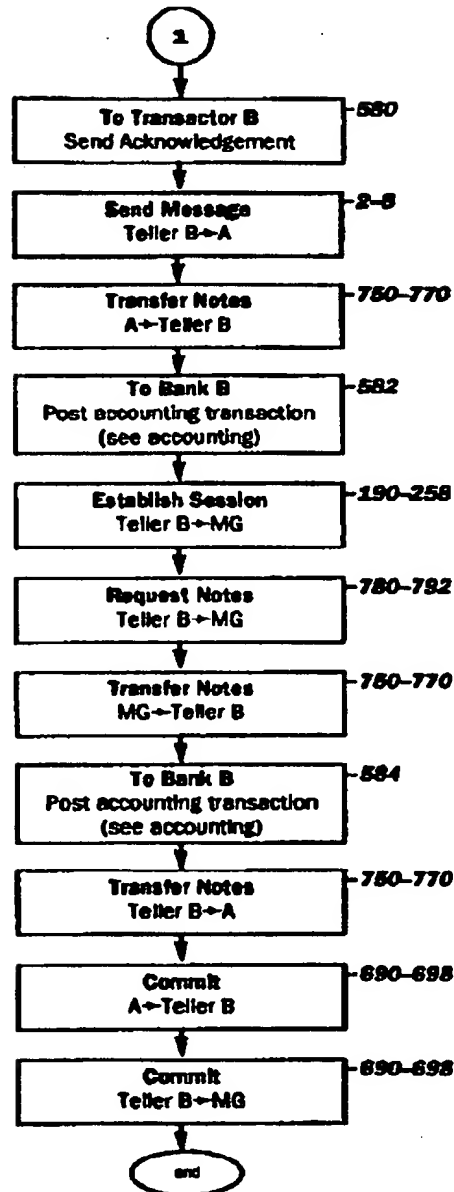


【図67】



Update Money Module Notes and Certificate

【図68】



Update Money Module Notes and Certificate (continued)

【手続補正書】

【提出日】平成5年2月10日

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 金銭の電子的象徴を用い、かつ少なくとも

1つの金融機関と前記金融機関により奉仕される加入者を含む通貨システムであって、
各々が前記電子的象徴を、それが象徴する金額及び前記電子的象徴の有効性を指示するデータを含む機械読取可能なデジタル型において収容できるようにした複数の加入者プロセッサと、
前記金融機関により用いられて前記加入者プロセッサと通信することにより、前記加入者プロセッサにストアさ

れた電子的象徴を前記金融機関に預金すること、又は前記加入者プロセッサに対し前記金融機関から前記電子的象徴を払い戻すことを可能にした処理手段とを備え、前記加入者プロセッサはさらに、加入者プロセッサ間において前記電子的象徴の交換を行うことができるようにするための通信及び処理機能を含むものであることを特徴とする通貨システム。

【請求項2】 前記金銭象徴物としての電子的象徴が銀行手形と同等に機能するものとして用いられることを特徴とする請求項1記載のシステム。

【請求項3】 前記システムが、前記電子的象徴の有効性を指示することによりその処理を可能にするための証明資源を含むことを特徴とする請求項1記載のシステム。

【請求項4】 前記システム中に複数の金融機関と、前記複数の金融機関及び前記加入者プロセッサ相互間で清算処理を行うための決済機関が含まれることを特徴とする請求項1記載のシステム。

【請求項5】 前記加入者プロセッサ中にストアされた前記データが、前記電子的象徴の状態を確認するためのデータ表現を含むことを特徴とする請求項1記載のシステム。

【請求項6】 前記加入者プロセッサ中にストアされた前記電子的象徴が、前記金融機関との取引中において更新された電子的象徴と置換されるようにしたことを特徴とする請求項1記載のシステム。

【請求項7】 経済的価値を安全確実に交換するために電子媒体を用いる通貨システムであって、信用認可の電子的象徴、及び銀行における営業性預金により支持された通貨の電子的象徴と、前記信用の電子的象徴及び前記通貨の電子的象徴を発生するための手段と、前記発生手段に結合されて前記信用及び通貨の前記電子的象徴を発行し、分配し、及び受け入れるための出納手段、及び前記信用及び通貨の電子的象徴をストアし、かつ移転するための取引手段であって、前記移転を他の取引手段との間及び前記手段と前記出納手段との間において実行することができるようにしたものを備えたことを特徴とする通貨システム。

【請求項8】 前記システムがさらに、その通貨システムの安全性及び完全性を維持するための安全保障手段を含むことを特徴とする請求項7記載のシステム。

【請求項9】 前記安全保障手段がさらに、前記取引手段間における前記信用及び通貨の電子的象徴の移転可能性に時間的制限を与えるものであることを特徴とする請求項8記載のシステム。

【請求項10】 前記発生手段、前記出納手段及び前記取引手段の各々が個々に認識番号を有し、前記安全保障手段がさらに、前記発生手段、前記出納手段及び前記取引手段の各々における前記認識番号の安全な証明を提供

するための証明手段を含むことを特徴とする請求項8記載のシステム。

【請求項11】 前記証明がさらに、前記発生手段、前記出納手段又は前記取引手段のうちの他のものによるその受入可能性の時間限度を含むようにしたことを特徴とする請求項10記載のシステム。

【請求項12】 前記安全保障手段がさらに、前記発生手段、前記出納手段、前記取引手段、及び前記安全保障手段の相互間における通信リンクを提供するためのネットワーク接続手段を含むことを特徴とする請求項8記載のシステム。

【請求項13】 前記発生手段がさらに、信用及び通貨のための電子的象徴を複数の通貨単位について発生するものであることを特徴とする請求項7記載のシステム。

【請求項14】 前記信用及び通貨のための電子的象徴が経済的価値として受け入れられるとともに、それらの初期の経済的価値以下の価値において通信及び移転されるものであることを特徴とする請求項7記載のシステム。

【請求項15】 前記信用の電子的象徴が前記取引手段により1回だけ移転されるようにしたこと特徴とする請求項14記載のシステム。

【請求項16】 前記発生手段がさらに、前記信用及び通貨のための電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項7記載のシステム。

【請求項17】 前記出納手段がさらに、前記信用及び通貨のための電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項7記載のシステム。

【請求項18】 前記取引手段がさらに、前記信用及び通貨のための電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項7記載のシステム。

【請求項19】 前記信用及び通貨のための電子的象徴が、

- (1) 通貨又は信用のいずれを表しているか、
 - (2) その移転可能性の時間限度、
 - (3) その経済的価値と前記電子的象徴をすでに記憶した他の取引手段、
 - (4) 前記発生手段の前記デジタル署名、
 - (5) 前記出納手段の前記デジタル署名、
 - (6) 前記他の取引手段における前記デジタル署名、
 - (7) 前記他の取引手段における前記証明、
 - (8) 前記出納手段における前記証明、
 - (9) 前記発生取引手段の前記証明、
 - (10) 前記通貨又は信用のための電子的象徴の認識番号、
- の表記を含むものであることを特徴とする請求項15記

載のシステム。

【請求項20】 前記発生手段、前記出納手段、及び前記取引手段が不正行為防止用ハウジングに収納されたプログラムブルデータ処理装置から構成されたものであることを特徴とする請求項7記載のシステム。

【請求項21】 前記発生手段、前記出納手段及び前記取引手段がコンピュータのモジュラ型共同プロセッサとして機能するように構成されたことを特徴とする請求項20記載のシステム。

【請求項22】 前記システムがさらに、2以上の手段により発行された信用及び通貨のための前記電子的象徴を清算するための手段を含むことを特徴とする請求項7記載のシステム。

【請求項23】 少くとも1つの金融機関により提供される通貨の電子的象徴又は信用の電子的象徴を用いる方法であって、前記金融機関が前記電子的象徴を発生する手段と、前記電子的象徴を発行し、かつ受け入れるとともに前記機関による加入者への奉仕を実行するための出納手段を有するものであり、前記方法が、

(1) 営業性預金により支持された通貨のための前記電子的象徴を発生するか、又は信用認可のための前記電子的象徴を発生するステップと、

(2) 前記通貨又は信用のための電子的象徴を前記加入者に対して発行するとともに、前記金融機関における前記出納手段から受け入れるステップ、及び

(3) 前記加入者に対し、前記通貨又は信用のために前記発行された電子的象徴を受け入れるとともに、その電子的象徴を前記取引手段を有する他の加入者及び前記出納手段に移転するための取引手段を提供するステップを含むことを特徴とする通貨又は信用のための電子的象徴を用いる方法。

【請求項24】 前記方法がさらに、前記通貨又は信用のための前記電子的象徴にデジタルサインを施し、これによってその複製もしくは変造等を防止して信頼性及び安全性を提供するステップを含むことを特徴とする請求項23記載の方法。

【請求項25】 前記方法がさらに、前記通貨又は信用のための前記電子的象徴が前記取引手段間において移転可能な時間周期を制限するステップを含むことを特徴とする請求項24記載の方法。

【請求項26】 前記方法がさらに、前記取引手段が前記金融機関と取引する限り、前記取引手段中にストアされた通貨を表す電子的象徴のすべてを取り除くステップと、移転可能性の時間限度を更新した通貨を表す新たな電子通貨を発生するステップ、及び前記取引手段において前記最初の通貨を表す電子的象徴を置換するステップを含むことを特徴とする請求項25記載の方法。

【請求項27】 前記方法がさらに、前記取引手段が前記信用の電子的象徴を発行する金融機関と取引するときに、前記取引手段中にストアされた信用を表す前記電子

的象徴のすべてを取り除くステップと、移転可能な時間限度を更新した新たな信用を表す電子的象徴を発生するステップ、及び前記取引手段において前記最初の信用を表す電子的象徴を置換するステップを含むことを特徴とする請求項25記載の方法。

【請求項28】 前記方法がさらに、前記金融機関により発行された通貨又は信用を表す前記電子的象徴のレコードを清算し、かつ維持するステップを含むことを特徴とする請求項23記載の方法。

【請求項29】 前記方法がさらに、前記発生手段、前記出納手段及び前記取引手段の各々に対し新規の認識番号を提供するステップを含むことを特徴とする請求項23記載の方法。

【請求項30】 前記方法がさらに、前記発生手段、前記出納手段及び前記取引手段の各々における所定時間内での前記認識番号の有効性を確認するステップを含むことを特徴とする請求項29記載の方法。

【請求項31】 前記方法がさらに、前記発生手段、前記出納手段及び前記取引手段の各々に対し、何らかの理由で好ましくない出納手段、発生手段、又は取引手段のリストを提供するステップを含むことを特徴とする請求項30記載の方法。

【請求項32】 前記方法がさらに、複数の異なった通貨単位について信用及び通貨を表す前記電子的象徴を発生するステップを含むことを特徴とする請求項23記載の方法。

【請求項33】 前記方法がさらに、前記金融機関において前記通貨又は信用を表す電子的象徴の分配、及び何らかの金融取引後における各金融機関の債務を監視するための会計構造を提供するステップを含むことを特徴とする請求項23記載の方法。

【請求項34】 前記方法がさらに、前記金融機関の各々において前記加入者に関連する口座のための個々のリストを前記取引手段にストアするステップを含むことを特徴とする請求項33記載の方法。

【請求項35】 前記方法がさらに、コルレス金融機関のデジタル署名により前記銀行口座のリストの各々にデジタル署名し、これによって前記口座に対する無権限者のアクセスを防止するためのステップを含むことを特徴とする請求項34記載の方法。

【請求項36】 前記方法がさらに、前記取引手段により実行された取引のレコードを維持するとともに、前記取引手段内の前記レコードをストアするステップを含むものであり、前記取引レコードが移転日、移転金額、前記通貨又は信用を表す電子的象徴を発行する金融機関の認識番号、前記取引に含まれる他の取引手段の認識番号、及び移転された通貨又は信用を表す電子的象徴の認識番号の表記を含むものであることを特徴とする請求項29記載の方法。

【請求項37】 前記方法がさらに、前記金融機関にお

ける前記取引レコードの複製を維持するステップと、前記手段のいずれかとの取引後において前記取引手段の各々に対する前記レコードを更新するステップを含むことを特徴とする請求項36記載の方法。

【請求項38】 前記方法がさらに、前記取引手段の前記取引レコードを、前記通貨及び信用を表す電子的象徴の清算により発生した取引レコードを用いて調整するステップを含むことを特徴とする請求項37記載の方法。

【請求項39】 前記方法がさらに、

- (1) 前記取引手段間で発生した個々の取引のレコードを、個別ストレージ手段にストアするステップと、
- (2) 前記通貨又は信用が、紛失し又は盗難に会った取引手段中にストアされている時に、前記ストレージ手段中にストアされた個々の取引に関する前記レコードを、前記金融機関に提出するステップと
- (3) 前記取引手段間における個々の取引の前記記録を前記通貨及び信用の前記電子的象徴の前記調整によって生じたレコードと比較することにより、前記紛失し又は盗難に会った取引手段中にストアされた通貨及び信用の電子的象徴の真の値を判定するステップ、を含むことを特徴とする請求項38記載の方法。

【請求項40】 前記方法がさらに、前記金融機関及び前記取引手段を互いに接続する通信ネットワークを提供するステップを含むことを特徴とする請求項23記載の方法。

【請求項41】 銀行における営業性預金により支持された通貨を表す電子的象徴を用いて取引を行うための電子通貨システムであって、前記通貨を表す電子的象徴を発生するための手段と、前記通貨を表す電子的象徴を発行し、かつ分配するための出納手段と、前記通貨を表す電子的象徴をストアし、かつ移転するための取引手段であって、前記移転を他の取引手段との間において実行する手段を備えたことを特徴とする電子通貨システム。

【請求項42】 信用認可を表す電子的象徴を用いて取引を行うための電子通貨システムであって、前記信用を表す電子的象徴を発生するための手段と、前記信用を表す電子的象徴を発行し、かつ分配するための出納手段と、

前記信用を表す電子的象徴をストアし、かつ移転するための取引手段であって、前記移転を他の取引手段との間及び前記取引手段と前記出納手段との間において実行する手段を備えたことを特徴とする電子通貨システム。

【請求項43】 前記システムがさらに、その電子通貨システムの安全性及び完全性を維持するための安全保障手段を含むことを特徴とする請求項41又は42記載のシステム。

【請求項44】 前記システムがさらに、前記発生手段、前記出納手段、前記取引手段、及び前記安全保障手

段間における通信ネットワークを提供するための手段を含むことを特徴とする請求項41又は42記載のシステム。

【請求項45】 前記システムがさらに、前記発生手段により発行された通貨又は信用を表す電子的象徴のレコード、及び前記取引手段により前記出納手段に移転された前記通貨又は信用を表す電子的象徴のレコードをストアするための口座データファイルを維持し、かつ処理するための手段を含むことを特徴とする請求項41又は42記載のシステム。

【請求項46】 前記安全保障手段がさらに、前記信用を表す電子的象徴及び前記通貨を表す電子的象徴の前記取引手段間における移転可能性の時間限度を設定するものであることを特徴とする請求項43記載のシステム。

【請求項47】 前記発生手段、前記出納手段及び前記取引手段の各々が個々に認識番号を有し、前記電子通貨システムの安全性を維持するための手段がさらに、前記発生手段、前記出納手段及び前記取引手段の各認識番号の独自の証明を行うための証明手段を含むことを特徴とする請求項43記載のシステム。

【請求項48】 前記証明がさらに、前記発生手段、前記出納手段もしくは前記取引手段のうちの他のものによるその受入可能な時間限度を含むことを特徴とする請求項47記載のシステム。

【請求項49】 前記発生手段がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項41又は42記載のシステム。

【請求項50】 前記出納手段がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項41又は42記載のシステム。

【請求項51】 前記取引手段がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴の上にデジタル署名を形成するためのパブリックキーデジタル形成手段を含むことを特徴とする請求項41又は42記載のシステム。

【請求項52】 前記通貨を表す電子的象徴又は前記信用を表す電子的象徴が経済的価値として受け入れられるものであることを特徴とする請求項41又は42記載のシステム。

【請求項53】 前記通貨を表す電子的象徴又は前記信用を表す電子的象徴が発生された初期の経済的価値に等しいか、又はそれ以下の値において通信及び移転されることを特徴とする請求項41又は42記載のシステム。

【請求項54】 前記信用を表す電子的象徴が前記取引手段により1回だけ移転可能であることを特徴とする請求項53記載のシステム。

【請求項55】 前記通貨を表す電子的象徴又は前記信用を表す電子的象徴がさらに、

- (1) その象徴が通貨又は信用のいずれを表しているか、
- (2) 前記移転可能なその時間限度、及び
- (3) その経済的価値

からなる表記を含むことを特徴とする請求項41又は42記載のシステム。

【請求項56】 前記表記がさらに、

- (1) 前記電子的象徴をすでにストアした他の発生手段、出納手段及び取引手段に関する表記、
- (2) 前記他の取引手段の証明、
- (3) 前記出納手段の証明、及び
- (4) 前記発生手段の証明

を含むことを特徴とする請求項55記載のシステム。

【請求項57】 前記表記がさらに、

- (1) 前記発生手段の前記デジタル署名、
- (2) 前記出納手段の前記デジタル署名、及び
- (3) 前記他の取引手段における前記デジタル署名の表記を含むことを特徴とする請求項56記載のシステム。

【請求項58】 前記発生手段、前記出納手段、及び前記取引手段が各々不正行為防止用ハウジングに収納されたプログラマブル処理装置からなることを特徴とする請求項41又は42記載のシステム。

【請求項59】 前記発生手段、前記出納手段、及び前記取引手段が汎用コンピュータのモジュラ型共同プロセッサとして機能するものであることを特徴とする請求項58記載のシステム。

【請求項60】 前記プログラマブル処理装置の各々がさらに、他の好ましくないプログラマブル処理装置のリ

ストを含んでいることを特徴とする請求項58記載のシステム。

【請求項61】 前記システムがさらに、2以上の出納手段により発行された信用及び通貨を表す電子的象徴を清算するための手段を含むことを特徴とする請求項41又は42記載のシステム。

【請求項62】 前記金融機関がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴の分配と、いずれかの金融取引後における各金融機関の負債を監視するための会計構造を含むことを特徴とする請求項41又は42記載のシステム。

【請求項63】 前記取引手段中における前記プログラマブル処理装置がさらに、前記異なった金融機関の各々において維持された前記取引手段の所有者に関する個々の口座リストを含むことを特徴とする請求項58記載のシステム。

【請求項64】 前記口座リストの各々がさらに、前記口座を維持する金融機関のデジタル署名を含むことにより、前記口座への無権限者のアクセスを防止することを特徴とする請求項63記載のシステム。

【請求項65】 前記発生手段がさらに、前記通貨を表す電子的象徴又は前記信用を表す電子的象徴を複数の通貨単位において発生するものであることを特徴とする請求項41又は42記載のシステム。

【請求項66】 前記プログラマブル処理装置の各々が、前記金融機関のいずれとも何らの関係を有しない個人であって、その存在認識に関して匿名性を維持したものにより個人的にコード化されることにより、無権限者によるその処理装置の使用を禁止するようにしたことを特徴とする請求項58記載のシステム。